NWD2105

Wireless N-lite USB Adapter

User's Guide

Version 1.0
Edition 1, 05/2010

ZyXEL

www.zyxel.com

Copyright © 2010
ZyXEL Communications Corporation

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the NWD2105 using the ZyXEL utility.

Tips for Reading User's Guides On-Screen

When reading a ZyXEL User's Guide On-Screen, keep the following in mind:

- If you don't already have the latest version of Adobe Reader, you can download it from http://www.adobe.com.
- Use the PDF's bookmarks to quickly navigate to the areas that interest you. Adobe Reader's bookmarks pane opens by default in all ZyXEL User's Guide PDFs.
- If you know the page number or know vaguely which page-range you want to view, you can enter a number in the toolbar in Reader, then press [ENTER] to jump directly to that page.
- Type [CTRL]+[F] to open the Adobe Reader search utility and enter a word or phrase. This can help you quickly pinpoint the information you require. You can also enter text directly into the toolbar in Reader.
- To quickly move around within a page, press the [SPACE] bar. This turns your cursor into a "hand" with which you can grab the page and move it around freely on your screen.
- Embedded hyperlinks are actually cross-references to related text. Click them to jump to the corresponding section of the User's Guide PDF.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

- Online Help

  Embedded web help for descriptions of individual screens and supplementary information.

- Support Disc

  Refer to the included CD for support documents.

Documentation Feedback

Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.

- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the documentation in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your NWD2105.

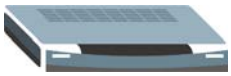
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The NWD2105 may be referred to as the "NWD2105", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons.

Wireless Access Point	Computer	Notebook computer
Server	Modem 	Telephone
Internet	Wireless Signal	

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Ground yourself (by properly using an anti-static wrist strap, for example) whenever working with the device's hardware or connections.
- ONLY qualified service personnel should service or disassemble this device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Contents Overview

Introduction and Configuration 15

Getting Started 17
Tutorial 23
Wireless LANs 37
Station Mode 49
AP Mode 75
Maintenance 85

Troubleshooting and Specifications 89

Troubleshooting 91
Product Specifications 95

Appendices and Index 99

Table of Contents

About This User's Guide **3**

Document Conventions **5**

Safety Warnings **7**

Contents Overview **9**

Table of Contents **11**

Part I: Introduction and Configuration **15**

Chapter 1
Getting Started **17**

1.1 Overview 17
1.1.1 What You Need to Know 17
1.1.2 Before You Begin 18
1.2 About Your NWD2105 18
1.2.1 Hardware 18
1.3 Application Overview 19
1.3.1 Infrastructure 19
1.3.2 Ad-Hoc 20
1.4 Hardware and Utility Installation 20
1.4.1 ZyXEL Utility Icon 20
1.5 Configuration Methods 21
1.5.1 Enabling Windows Wireless Configuration 21
1.5.2 Accessing the ZyXEL Utility 21

Chapter 2
Tutorial **23**

2.1 Overview 23
2.1.1 What You Can Do in This Tutorial 23
2.1.2 What You Need to Know 23
2.1.3 Before You Begin 24
2.2 Connecting to an AP using Wi-Fi Protected Setup (WPS) 24
2.2.1 Push Button Configuration (PBC) 24
2.2.2 PIN Configuration 25
2.3 Connecting to an AP Without Using WPS 29

2.3.1 Manually Connecting to a Wireless LAN 29
2.3.2 Creating and Using a Profile 31
2.4 Configuring the NWD2105 as an AP 34

Chapter 3
Wireless LANs 37

3.1 Overview 37
3.1.1 What You Can Do in This Section 37
3.1.2 What You Need to Know 37
3.1.3 Before You Begin 38
3.2 Wireless LAN Overview 38
3.3 Wireless LAN Security 39
3.3.1 User Authentication and Encryption 39
3.4 WiFi Protected Setup 41
3.4.1 Push Button Configuration 42
3.4.2 PIN Configuration 42
3.4.3 How WPS Works 44
3.4.4 Limitations of WPS 47

Chapter 4
Station Mode 49

4.1 Overview 49
4.1.1 What You Can Do in This Section 49
4.1.2 What You Need to Know 49
4.1.3 Before You Begin 50
4.2 ZyXEL Utility Screen Summary 50
4.3 The Link Info Screen 51
4.3.1 Trend Chart 53
4.4 The Site Survey Screen 54
4.4.1 Security Settings 55
4.4.2 Summary Screen 61
4.5 The Profile Screen 62
4.5.1 Adding a New Profile 64
4.6 The Adapter Screen 68
4.6.1 WPS: PBC (Push Button Configuration) 69
4.6.2 WPS: PIN - Use this Device's PIN 69
4.6.3 WPS: PIN - Use the PIN from the AP or Wireless Router 70
4.7 Security Settings in Windows Vista 71
4.7.1 Using PEAP in Vista 72
4.7.2 Using TLS in Vista 73

Chapter 5
AP Mode 75

5.1 Overview 75
5.1.1 What You Can Do in This Section 76
5.1.2 What You Need to Know 76
5.1.3 Before You Begin 77
5.2 AP Mode Screen Summary 77
5.3 The Link Info Screen 78
5.4 The Configuration Screen 79
5.4.1 Security Settings 80
5.5 The MAC Filter Screen 83

Chapter 6
Maintenance 85

6.1 Overview 85
6.1.1 What You Can Do in This Section 85
6.1.2 What You Need to Know 85
6.1.3 Before You Begin 85
6.2 The About Screen 86
6.3 Uninstalling the ZyXEL Utility 86
6.4 Upgrading the ZyXEL Utility 87

Part II: Troubleshooting and Specifications 89

Chapter 7
Troubleshooting 91

7.1 Power, Hardware Connections, and LEDs 91
7.2 Accessing the ZyXEL Utility 92
7.3 Link Quality 92
7.4 Problems Communicating with Other Computers 93

Chapter 8
Product Specifications 95

Part III: Appendices and Index 99

Appendix A Setting Up Your Computer's IP Address 101

Appendix B Wireless LANs 131

Appendix C Windows Wireless Management 147

Appendix D Wireless for Windows 7 173

Appendix E Legal Information 179

Index..... 185

PART I
Introduction and Configuration

Getting Started (17)

Tutorial (23)

Wireless LANs (37)

Station Mode (49)

AP Mode (75)

Maintenance (85)

1

Getting Started

1.1 Overview

The ZyXEL NWD2105 wireless N-lite USB adapter brings you a better Internet experience over existing 802.11 networks. With data rates of up to 150 Mbps, you can enjoy a breathtaking high-speed connection at home or in the office. It is an excellent solution for daily activities such as file transfers, music downloading, video streaming and online gaming.

This section includes:

- About Your NWD2105 on page 18
- Application Overview on page 19
- Hardware and Utility Installation on page 20
- Configuration Methods on page 21

1.1.1 What You Need to Know

The following terms and concepts may help as you read through this section, and subsequently as you read through the rest of the User's Guide.

Access Point

An Access Point (AP) is a network device that acts as a bridge between a wired and a wireless network. Outside of the home or office, APs can most often be found in coffee shops, bookstores and other businesses that offer wireless Internet connectivity to their customers.

Infrastructure

An infrastructure network is one that seamlessly combines both wireless and wired components. One or more APs often serve as the bridge between wireless and wired LANs.

Ad-Hoc

An Ad-Hoc wireless LAN is a self-contained group of computers connected wirelessly and which is independent of any other networks and Access Points.

1.1.2 Before You Begin

- Read the Quick Start Guide for information on making hardware connections and using the ZyXEL utility to connect your NWD2105 to a network.

1.2 About Your NWD2105

Your NWD2105 is an IEEE 802.11n compliant wireless LAN adapter. It can also connect to IEEE 802.11b/g wireless networks. The NWD2105 is WPS (Wi-Fi Protected Setup) compliant. WPS allows you to easily connect to another WPS-enabled device.

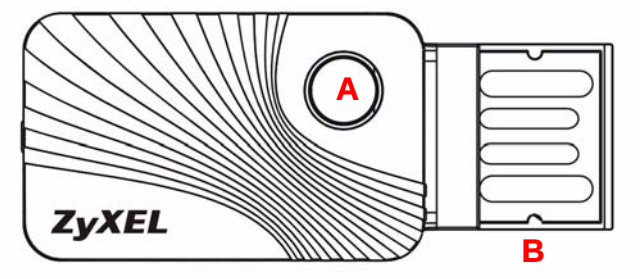
The NWD2105 is a USB adapter which connects to an empty USB port on your computer.

See your NWD2105's Quick Start Guide for installation instructions, and see the section on product specifications in this User's Guide for detailed information.

1.2.1 Hardware

This section describes the NWD2105's physical appearance.

Figure 1 The NWD2105



The following table describes the NWD2105.

Table 1 NWD2105 External View

LABEL	DESCRIPTION
A	LED and also a WPS button
B	USB connector

The following table describes the operation of the NWD2105's LEDs.

Table 2 NWD2105 LEDs

LED	COLOR	STATUS	DESCRIPTION
	Orange	Slow Blinking	The NWD2105 is turned on, connected to an AP, and is not transmitting or receiving data.
		Rapid Blinking	The NWD2105 is turned on, connected to an AP, and is transmitting or receiving data. It also blinks when the WPS feature is being used or a WPS connection is being initiated.
		Off	The NWD2105 is turned off.

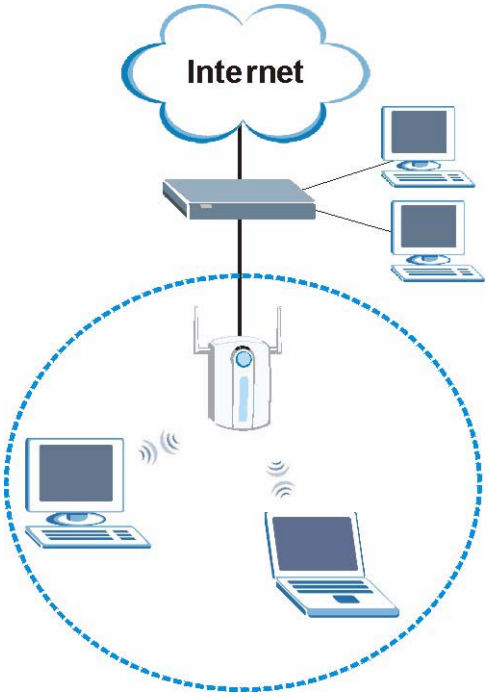
1.3 Application Overview

This section describes some network applications for the NWD2105. You can either set the network type to **Infrastructure** and connect to an AP or use **Ad-Hoc** mode and connect to a peer computer (another wireless device in Ad-Hoc mode).

1.3.1 Infrastructure

To connect to a network via an access point (AP), set the NWD2105 network type to **Infrastructure** (see Chapter 4 on page 62). Through the AP, you can access the Internet or the wired network behind the AP.

Figure 2 Application: Infrastructure



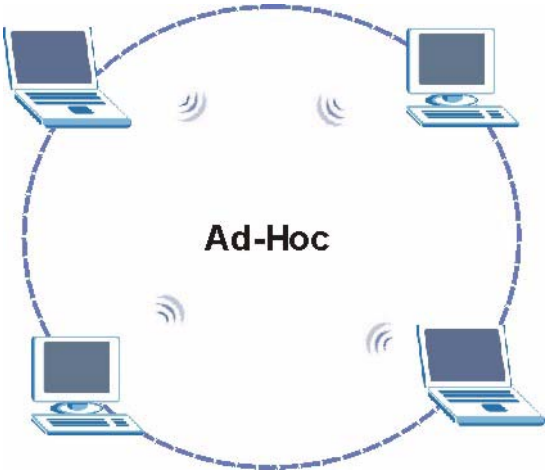
1.3.2 Ad-Hoc

To set up a small independent wireless workgroup without an AP, use **Ad-Hoc** (see Chapter 4 on page 62).

Ad-Hoc does not require an AP or a wired network. Two or more wireless clients communicate directly with each other.

Note: Wi-Fi Protected Setup (WPS) is not available in ad-hoc mode.

Figure 3 Application: Ad-Hoc



1.4 Hardware and Utility Installation

Follow the instructions in the Quick Start Guide to install the ZyXEL utility and make hardware connections.

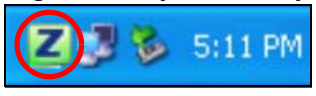
1.4.1 ZyXEL Utility Icon

After you install and start the ZyXEL utility, an icon for the ZyXEL utility appears in the system tray.

Note: The ZyXEL utility system tray icon displays only when the NWD2105 is installed properly.

Note: When you use the ZyXEL utility, it automatically disables Wireless Zero Configuration (WZC) in Windows XP.

Figure 4 ZyXEL Utility: System Tray Icon



The color of the ZyXEL utility system tray icon indicates the status of the NWD2105. Refer to the following table for details.

Table 3 ZyXEL Utility: System Tray Icon

COLOR	DESCRIPTION
Red	The NWD2105 is not connected to a wireless network.
Green	The NWD2105 is connected to a wireless network.

1.5 Configuration Methods

To configure your NWD2105, use one of the following applications:

- Wireless Zero Configuration (WZC, the Windows XP wireless configuration tool) or WLAN AutoConfig (the Windows Vista wireless configuration tool).
- The ZyXEL utility.

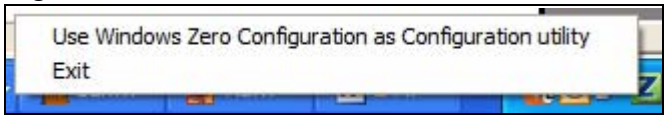
Note: Do NOT use Windows XP's Wireless Zero Configuration tool at the same time you use the ZyXEL utility.

1.5.1 Enabling Windows Wireless Configuration

Note: When you use the ZyXEL utility, it automatically disables Windows XP's wireless configuration tool.

If you want to use the Windows XP wireless configuration tool to configure the NWD2105, you need to disable the ZyXEL utility. Right-click the utility icon ( ) in the system tray and select **Exit**.

Figure 5 Enable WZC



Refer to the appendices for information on how to use the Windows wireless configuration tool to manage the NWD2105.

To reactivate the ZyXEL utility, double-click the ( ) icon on your desktop or click **Start** > **(All) Programs** > **Wireless N-lite USB Adapter Utility** > **Wireless N USB Adapter Utility**.

1.5.2 Accessing the ZyXEL Utility

Double-click on the ZyXEL wireless LAN utility icon in the system tray to open the ZyXEL utility.

The ZyXEL utility screens are similar in all Microsoft Windows versions. Screens for Windows XP are shown in this User's Guide.

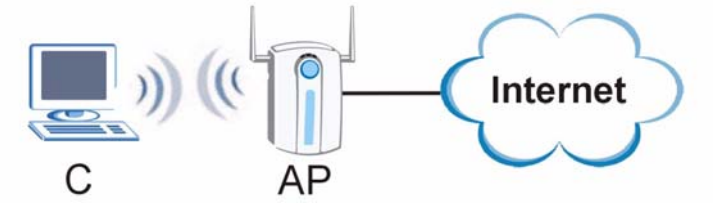
Note: Click the icon (located in the top right corner) to display the online help window.

2 Tutorial

2.1 Overview

This tutorial shows you how to join a wireless infrastructure network using the ZyXEL utility. The wireless client is labeled **C** and the Access Point is labeled **AP**.

Figure 6 Infrastructure Network



2.1.1 What You Can Do in This Tutorial

- Connect securely either to an infrastructure AP using the WPS protocol. See Section 2.2 on page 24 for details.
- Connect securely to an infrastructure AP using many of the strongest and most common encryption protocols. See Section 2.3 on page 29 for details.
- Save a your settings so that you can later connect again to an infrastructure AP with a single click. See Section 2.3.2 on page 31 for details.
- Configure your NWD2105 as an Access Point (AP), allowing other devices to connect to it and share its network connections. See Section 2.4 on page 34 for details.

2.1.2 What You Need to Know

The following term may help as you read through this section.

WPS

Wi-Fi Protected Setup (WPS) is a security protocol that lets two or more devices connect securely to one another with a minimum amount of hassle on your part. It most cases, establishing a secure connection with another WPS device is as easy as pushing a button.

2.1.3 Before You Begin

- Make sure that you have already familiarized yourself with the NWD2105's features and hardware, as described in Chapter 1 on page 17.
- You should have valid login information for an existing network Access Point, otherwise you may not be able to make a network connection right away.

2.2 Connecting to an AP using Wi-Fi Protected Setup (WPS)

This section gives you an example of how to set up your wireless network using WPS. This example uses the NWD2105 as the wireless client, and ZyXEL's NBG334W as the Access Point (AP).

Note: The Access Point must be a WPS-aware device.

There are two WPS methods for creating a secure connection. This tutorial shows you both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See Section 2.2.1 on page 24.This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the NWD2105's interface. See Section 2.2.2 on page 25. This is the more secure method, since one device can authenticate the other.

2.2.1 Push Button Configuration (PBC)

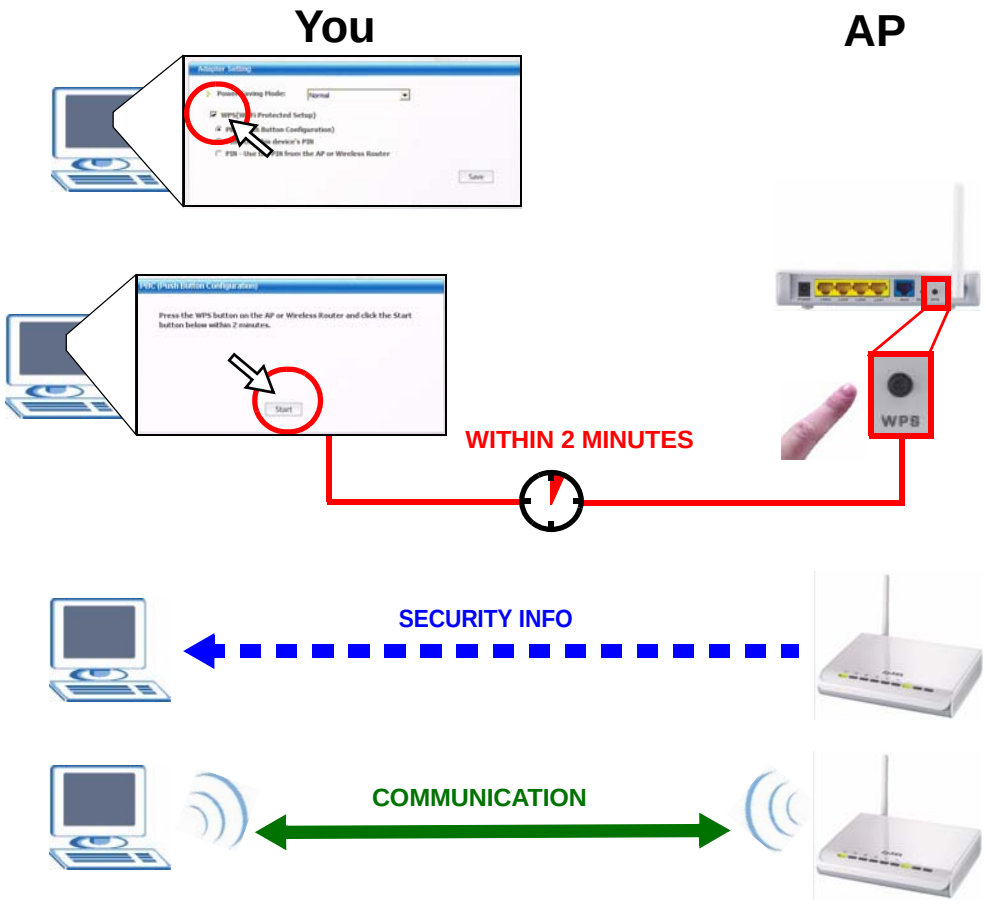
1. Make sure that your access point is turned on and that it is within range of the computer with the NWD2105 installed.
2. Make sure that you have installed the NWD2105's driver and utility on your computer.
3. In the NWD2105's utility, click the **Adapter** tab, enable **WPS** and select **PBC (Push Button Configuration)**. In the screen that appears, click **Start**.
4. Log into the AP's web configurator and locate its WPS settings section. On the NBG334W, press the **Push Button** button in the **Network** > **Wireless Client** > **WPS Station** screen.

   Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The AP sends the proper configuration settings to the NWD2105. This may take up to two minutes. Then the NWD2105 is able to communicate with the AP securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both the AP (the NBG334W in this example) and the NWD2105.

Figure 7 Example WPS Process: PBC Method



2.2.2 PIN Configuration

When you use the PIN configuration method, you need to use both the NWD2105's utility and the AP's configuration interface.

1 In the NWD2105's Adaptor tab, select **WPS** and **PIN - Use this Device's PIN**. Note down the PIN in the screen that appears.

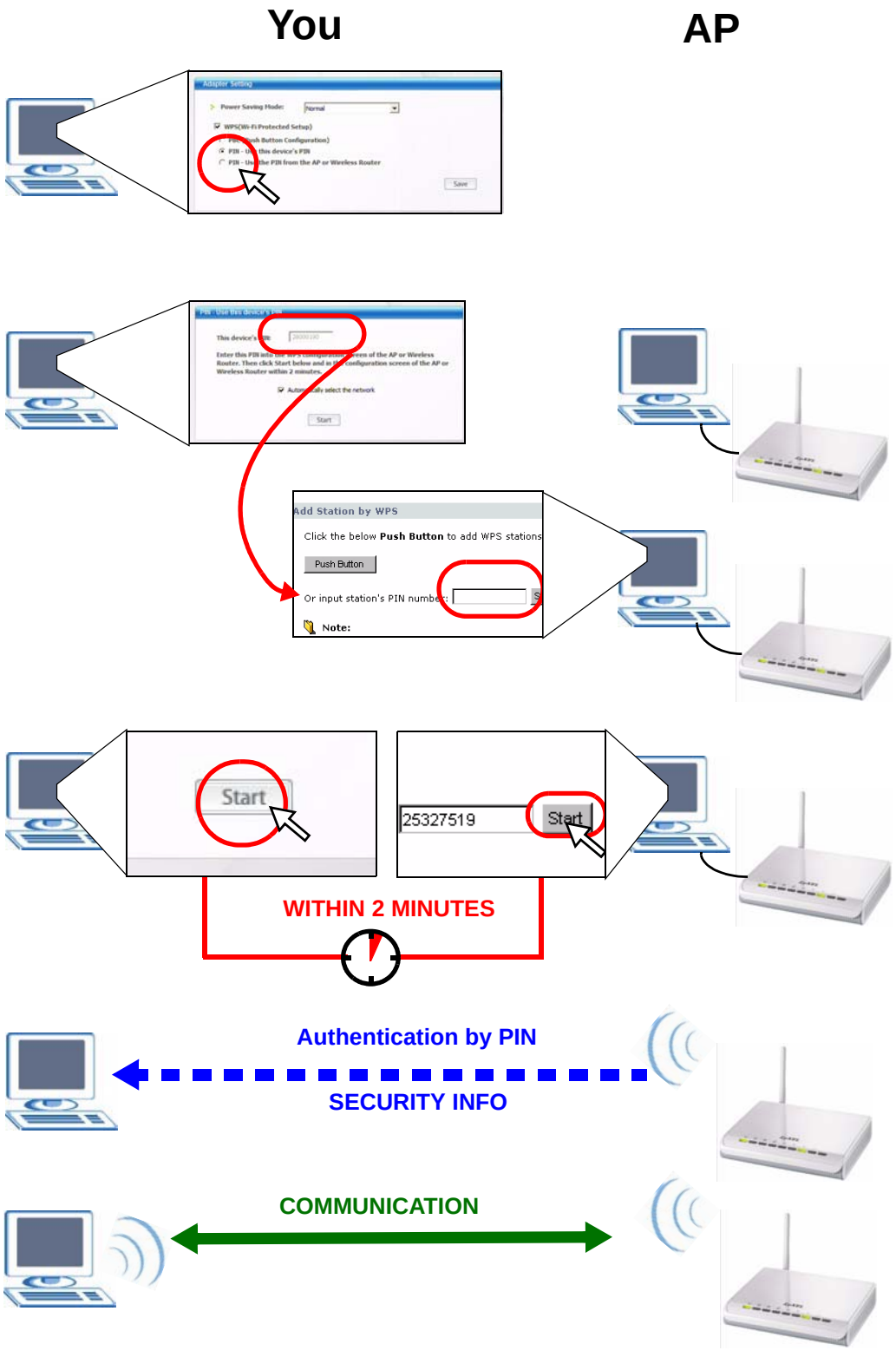
2 Enter the PIN number in the AP's configuration interface. In the NBG334W, use the **PIN** field in the **Network** > **Wireless LAN** > **WPS Station** screen.

3 Click the **Start** buttons on both the NWD2105 utility screen and the AP's configuration utility (the **WPS Station** screen on the NBG334W) within two minutes.

The NBG334W authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the NBG334W securely.

The following figure shows you the example of configuring the wireless network and security on the NWD2105 and the AP (ZyXEL's NBG334W in this example) by using the PIN method.

Figure 8 Example WPS Process: PIN Method



2.3 Connecting to an AP Without Using WPS

There are three ways to connect the wireless client (the NWD2105) to a network without using WPS.

- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network (see Section 2.3.1 on page 29).
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer (see Section 2.3.2 on page 31).

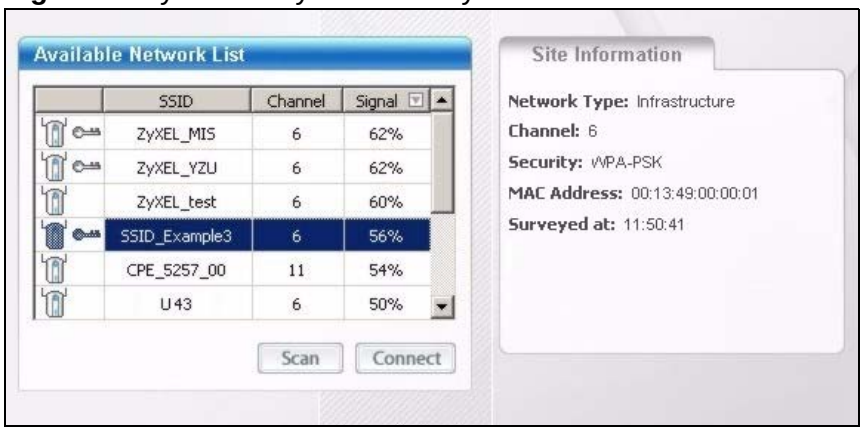
2.3.1 Manually Connecting to a Wireless LAN

This example illustrates how to manually connect your wireless client to an access point (AP) configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the AP's SSID is "SSID_Example3" and its pre-shared key is "ThisismyWPA-PSKpre-sharedkey".

After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.

Figure 9 ZyXEL Utility: Site Survey



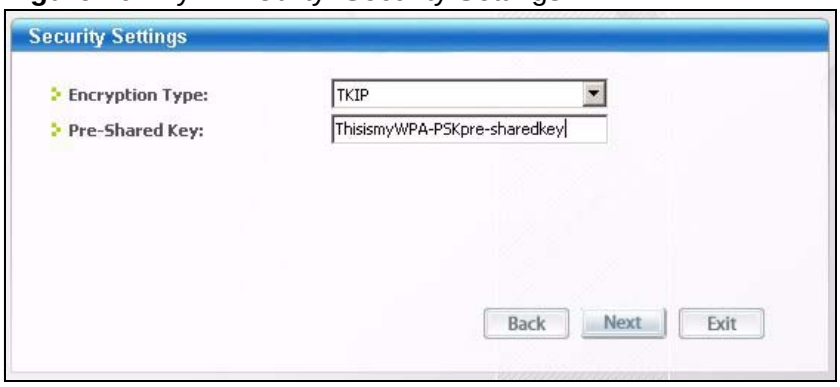
2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on, or move the wireless client closer to the AP or peer computer. See Table 4.4 on page 54 for detailed field descriptions.

3 To connect to an AP or peer computer, either click an entry in the list and then click **Connect** or double-click an entry (**SSID_Example3** in this example).

4 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

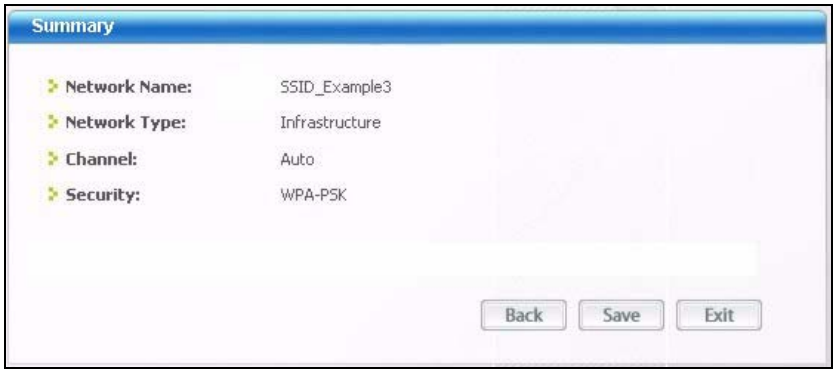
Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

Figure 10 ZyXEL Utility: Security Settings



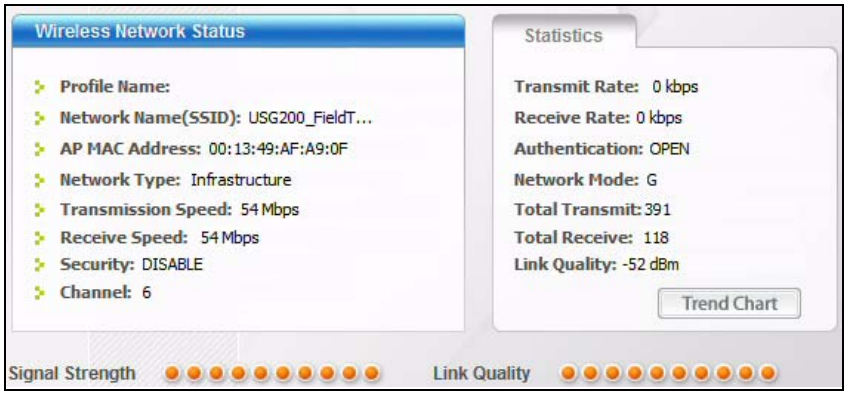
5 The **Summary** window appears. Check your settings and click **Save** to continue.

Figure 11 ZyXEL Utility: Summary



6 The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank. See Table 4.3 on page 51 for detailed field descriptions.

Figure 12 ZyXEL Utility: Link Info



7 Open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured. If you cannot access the web site, check the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

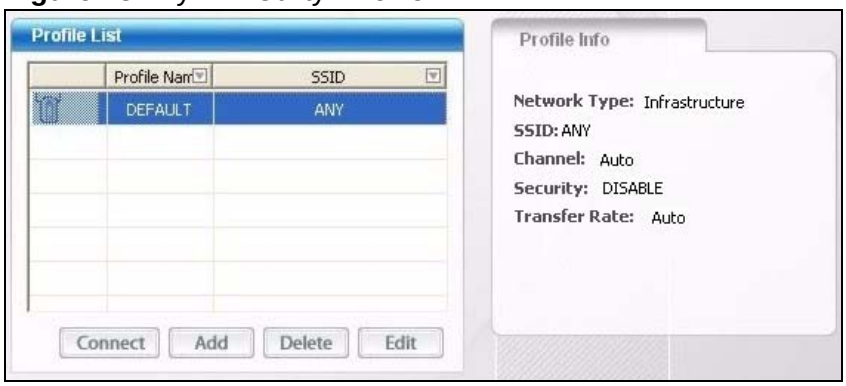
2.3.2 Creating and Using a Profile

A profile lets you automatically connect to the same wireless network every time you use the ZyXEL utility. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an access point configured for WPA-PSK security. In this example, the AP's SSID is "SSID_Example3" and its pre-shared key is "ThisismyWPA-PSKpre-sharedkey". You have chosen the profile name "PN_Example3".

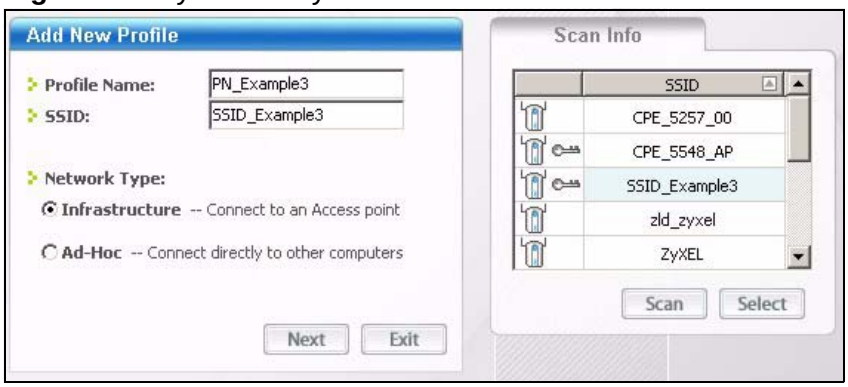
1 Open the ZyXEL utility and click the **Profile** tab to open the screen as shown. Click **Add** to configure a new profile.

Figure 13 ZyXEL Utility: Profile



2 The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, which are displayed in the **Scan Info** box. You can also configure your profile for a wireless network that is not in the list.

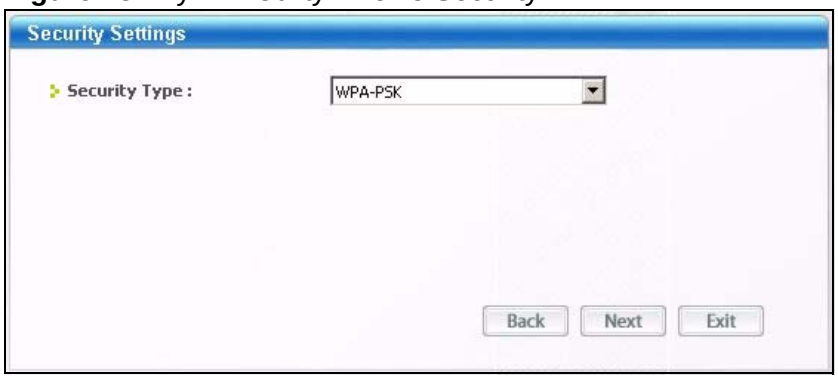
Figure 14 ZyXEL Utility: Add New Profile



3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.

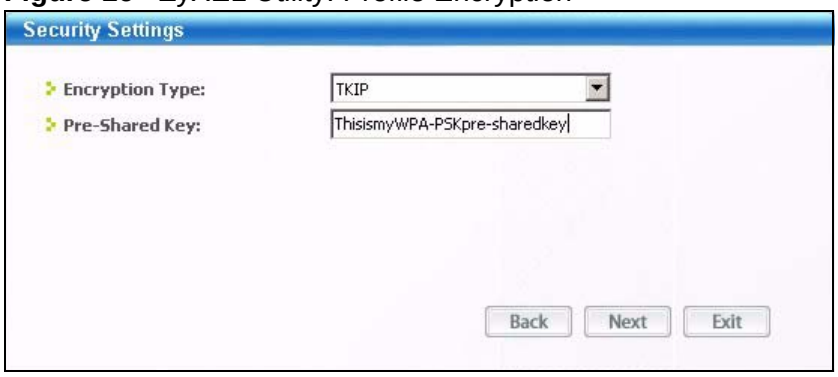
4 Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).

Figure 15 ZyXEL Utility: Profile Security



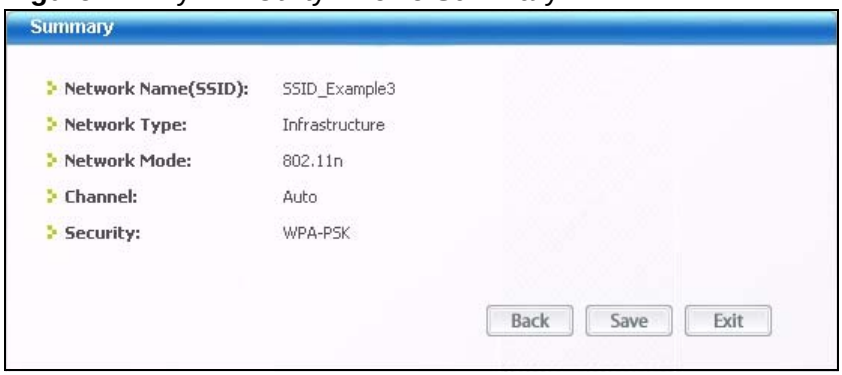
5 This screen varies depending on the encryption method you selected in the previous screen. In this example, enter the pre-shared key and leave the encryption type at the default setting.

Figure 16 ZyXEL Utility: Profile Encryption



6 Verify the profile settings in the ready-only screen. Click **Save** to save and go to the next screen.

Figure 17 ZyXEL Utility: Profile Summary



7 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button to go back to the **Profile List** screen.

If you clicked **Activate Later** you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.

Note: Only one profile can be activated and used at any given time.

Figure 18 ZyXEL Utility: Profile Activate

8 When you activate the new profile, the ZyXEL utility goes to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.

9 Make sure the selected AP in the active profile is on and connected to the Internet. Open your Internet browser, enter http://www.zyxel.com or the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.

10 If you cannot access the Internet, go back to the **Profile** screen. Select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

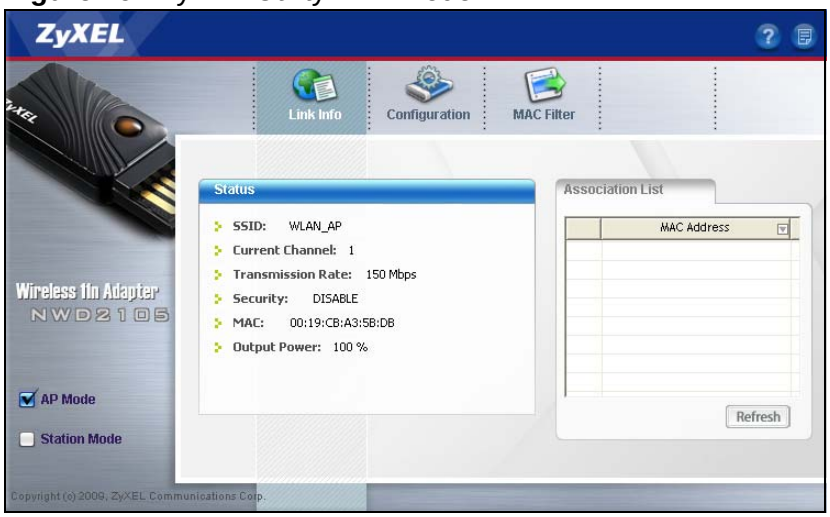
2.4 Configuring the NWD2105 as an AP

In access point mode, your NWD2105 allows you to set up your wireless network without using a dedicated AP. See Chapter 5 on page 75 for more information.

After you install the ZyXEL Utility and then connect the NWD2105 to your computer, follow the steps below to set up your NWD2105 as an AP.

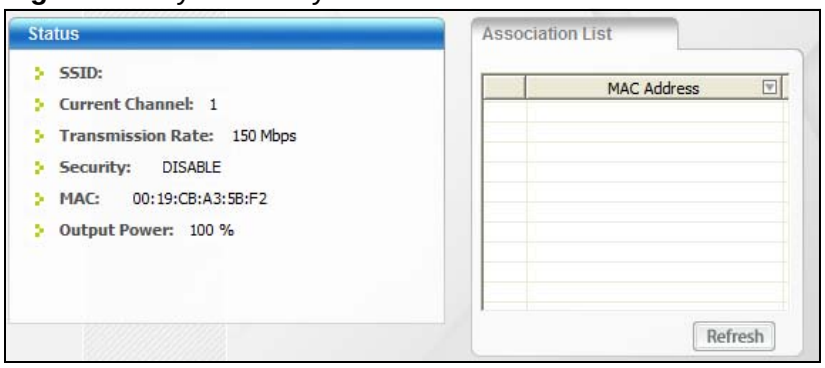
1 Select **AP Mode** in the main ZyXEL Utility screen. The **AP Mode** version of the default **Link Info** screen displays.

Figure 19 ZyXEL Utility - AP Mode



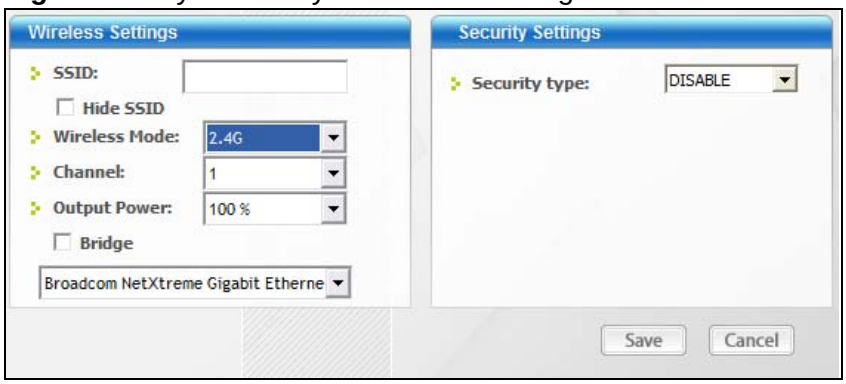
2 Under **Status**, you can view the current settings on the NWD2105. In the **Association List**, you can see if any wireless clients have connected to your NWD2105.

Figure 20 ZyXEL Utility - AP Mode: Link Info



3 If you want to change the access point's SSID and enable wireless security for your NWD2105, click the **Configuration** tab. See Section 5.4.1 on page 80 for detailed field descriptions found on this screen.

Figure 21 ZyXEL Utility - AP Mode: Configuration



3

Wireless LANs

3.1 Overview

This section provides background information on wireless Local Area Networks.

3.1.1 What You Can Do in This Section

- Connect securely to an AP using many of the strongest and most common encryption protocols. See Section 3.3 on page 39 for details.
- Connect securely either to an AP or computer-to-computer using WPS. See Section 3.4 on page 41 for details.

3.1.2 What You Need to Know

The following terms and concepts may help as you read through this section.

Server

When two or more devices are connected digitally to form a network, the one that distributes data to the other devices is known as the “server”. A RADIUS (Remote Authentication Dial-In User Service) is a kind of server that manages logins and logout, among other things, for the network to which it is connected.

Client

When two or more devices are connected digitally to form a network, the one that contacts and obtains data from a server is known as the “client”. Each client is designed to work with one or more specific kinds of servers, and each server requires a specific kind of client. Wireless adapters are clients that connect to a network server through an AP.

Authentication

Authentication is the process of confirming a client’s or user’s digital identity when they connect to a network. Turning off authentication means disabling all security protocols and opening your network to anyone with the means to connect to it.

Encryption

The process of taking data and encoding it, usually using a mathematical formula, so that it becomes unreadable unless decrypted with the proper code or pass phrase.

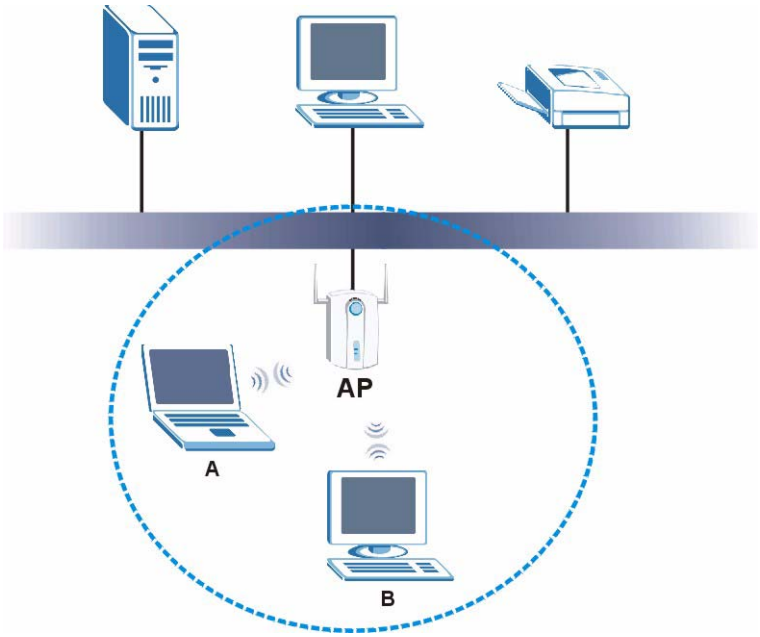
3.1.3 Before You Begin

- You should have valid login information for an existing network Access Point, otherwise you may not be able to make a network connection right away.

3.2 Wireless LAN Overview

The following figure provides an example of a wireless network with an AP. See Figure 3 on page 20 for an Ad Hoc network example.

Figure 22 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.

- If two wireless networks overlap, they should use a different channel.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every device in the same wireless network must use security compatible with the AP or peer computer.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

3.3 Wireless LAN Security

Wireless LAN security is vital to your network to protect wireless communications.

If you do not enable any wireless security on your NWD2105, the NWD2105's wireless communications are accessible to any wireless networking device that is in the coverage area.

Note: You can use only WEP encryption if you set the NWD2105 to Ad-hoc mode.

See the appendices for more detailed information about wireless security.

3.3.1 User Authentication and Encryption

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

3.3.1.1 WEP

3.3.1.1.1 Data Encryption

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the NWD2105 and the AP or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

There are two ways to create WEP keys in your NWD2105.

- Automatic WEP key generation based on a “password phrase” called a passphrase. The passphrase is case sensitive. You must use the same passphrase for all WLAN adapters with this feature in the same WLAN.

  For WLAN adapters without the passphrase feature, you can still take advantage of this feature by writing down the four automatically generated WEP keys from the **Security Settings** screen of the ZyXEL utility and entering them manually as the WEP keys in the other WLAN adapter(s).

- Enter the WEP keys manually.

  Your NWD2105 allows you to configure up to four 64-bit or 128-bit WEP keys. Only one key is used as the default key at any one time.

3.3.1.1.2 Authentication Type

The IEEE 802.11b/g standard describes a simple authentication method between the wireless stations and AP. Three authentication types are defined: **Auto**, **Open** and **Shared**.

- **Open** mode is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key. Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.
- **Shared** mode involves a shared secret key to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.
- **Auto** authentication mode allows the NWD2105 to switch between the open system and shared key modes automatically. Use the auto mode if you do not know the authentication mode of the other wireless stations.

3.3.1.2 IEEE 802.1x

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using an external RADIUS server.

3.3.1.2.1 EAP Authentication

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. The NWD2105 supports EAP-TLS, EAP-TTLS (at the time of writing, TTLS is not available in Windows Vista) and EAP-PEAP. Refer to Appendix B on page 131 for descriptions.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). Certificates (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

3.3.1.3 WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

3.4 WiFi Protected Setup

Your NWD2105 supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device’s documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

3.4.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within wireless range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the NWD2105, see Section 4.6.1 on page 69).
3. Press the button on one of the devices (it doesn't matter which).
4. Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

   If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

3.4.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you

need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

1 Ensure WPS is enabled on both devices.

2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.

3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the NWD2105, see Section 4.6 on page 68).

4 Enter the client's PIN in the AP's configuration interface.

Note: If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.

5 Start WPS on both devices within two minutes.

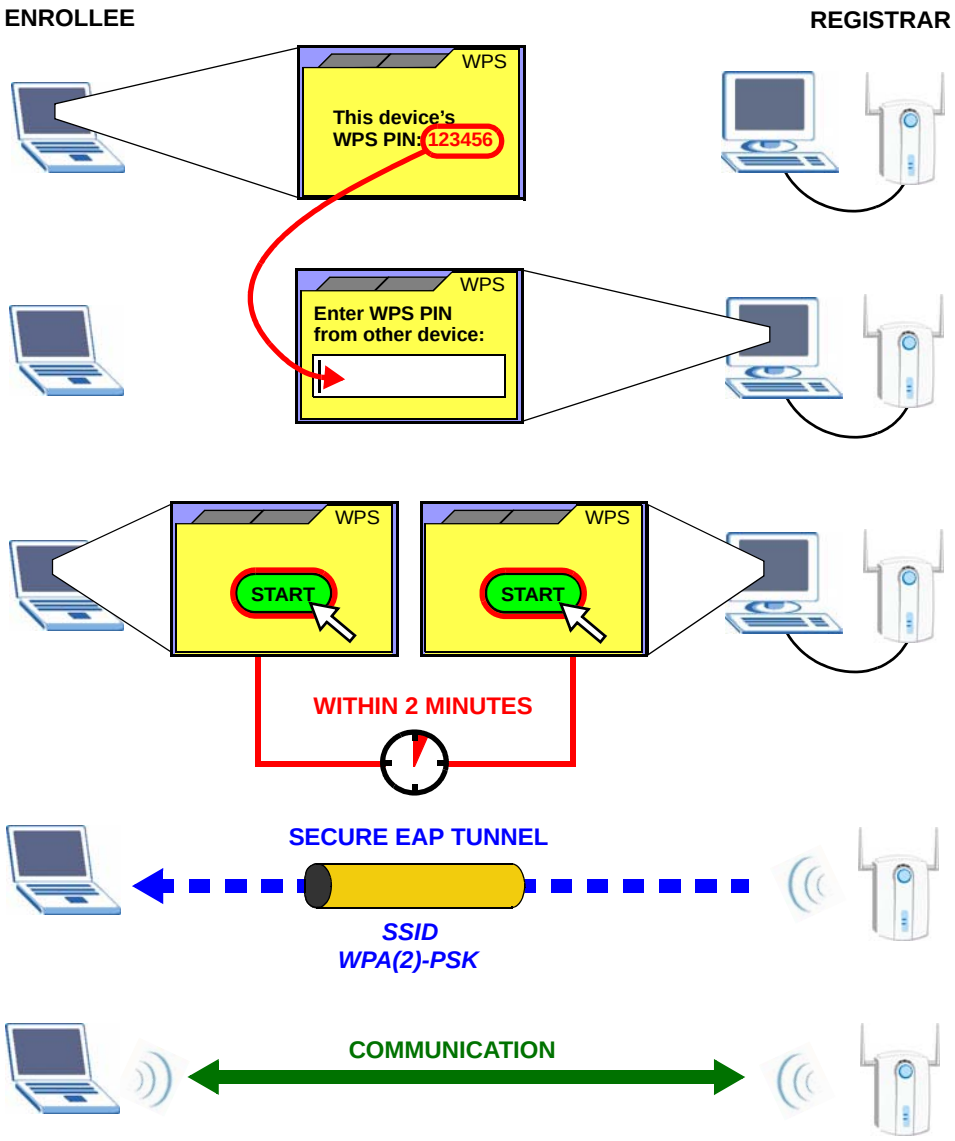
Note: Use the configuration utility to activate WPS, not the push-button on the device itself.

6 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 23 Example WPS Process: PIN Method



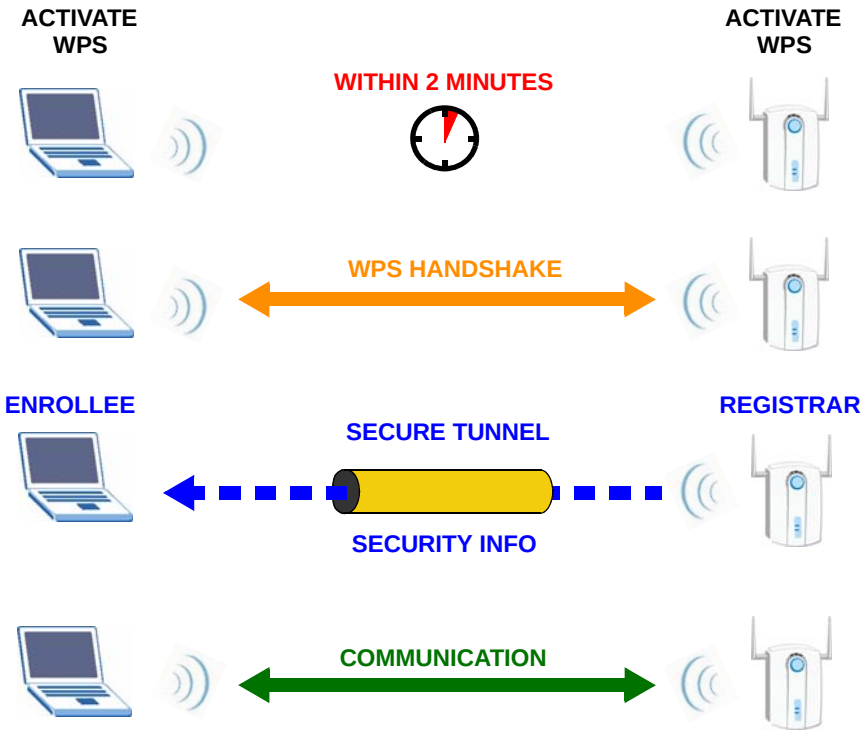
3.4.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is

already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 24 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

By default, a WPS devices is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all

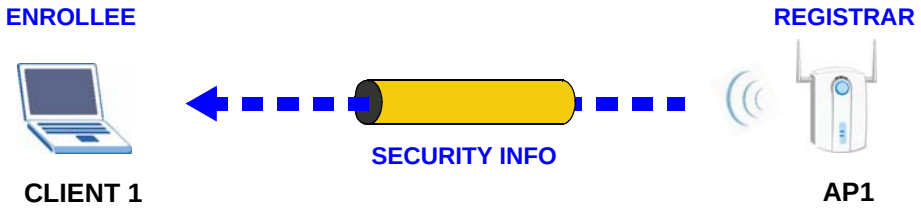
subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

3.4.3.1 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

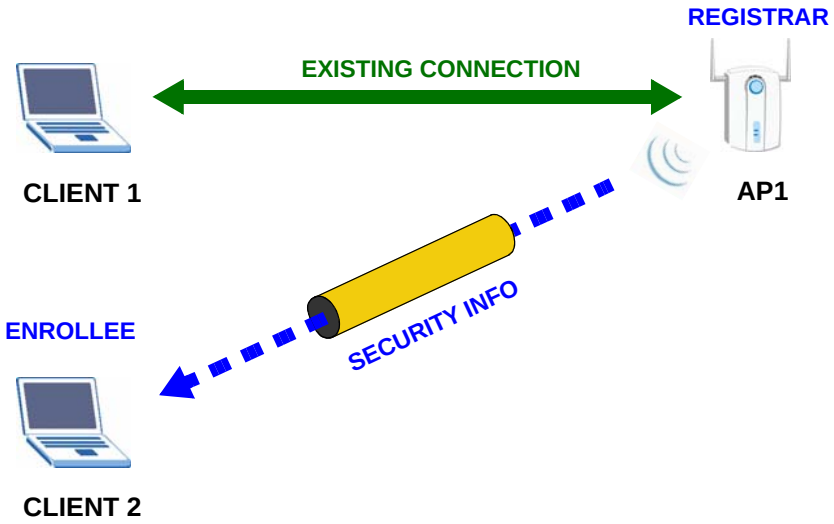
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 25 WPS: Example Network Step 1



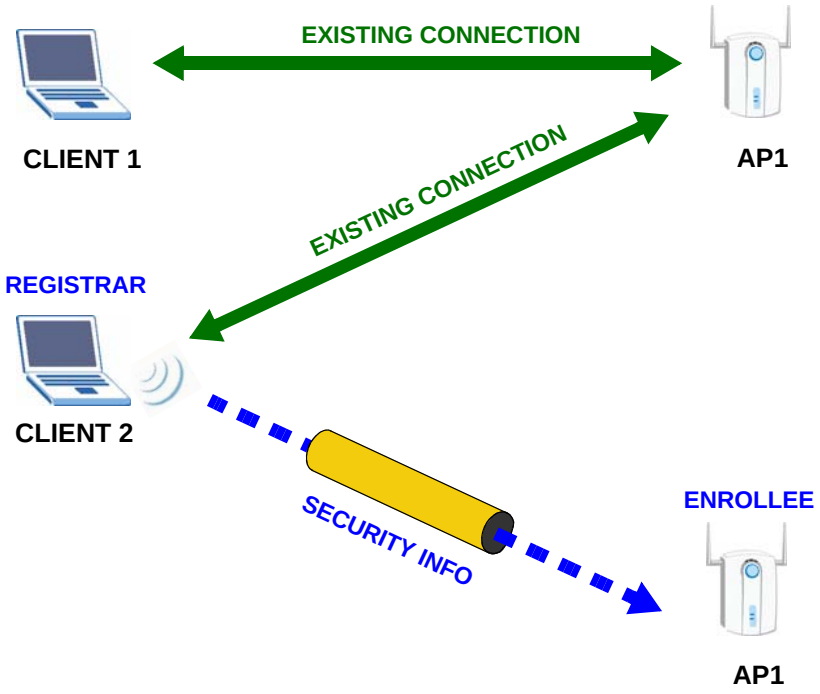
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 26 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 27 WPS: Example Network Step 3



3.4.4 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices (see Section 4.4.1.3 on page 57 for information on pre-shared keys). Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the

configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point’s configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

4

Station Mode

4.1 Overview

This section shows you how to configure your NWD2105 using the ZyXEL utility in Windows.

Note: Some features available in Windows XP or Windows 2000 are not available in Windows Vista.

4.1.1 What You Can Do in This Section

- On the **Link Info** screen, you can see your current connection details, monitor signal strength and quality, and more. See Section 4.3 on page 51 for details.
- On the **Site Survey** screen, you can connect to any available unsecured wireless network in range of the NWD2105, or open the security settings screen for any secured wireless network in range. See Section 4.4 on page 54 for details.
- On the **Profile** screen, you can create, delete and manage your wireless network profiles. See Section 4.5 on page 62 for details.
- On the **Adapter** screen, you can configure the NWD2105 hardware, such as activating WPS mode or its power saving feature. See Section 4.6 on page 68 for details.

4.1.2 What You Need to Know

The following terms and concepts may help as you read through this section.

Wired Equivalent Privacy (WEP)

WEP (Wired Equivalent Privacy) encrypts data transmitted between wired and wireless networks to keep the transmission private. Although one of the original wireless encryption protocols, WEP is also the weakest. Many people use it strictly to deter unintentional usage of their wireless network by outsiders.

Wi-fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. It improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA uses Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP. WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. The WPA protocol affords users with vastly stronger security than the WEP protocol. It comes in two different varieties: WPA and WPA2. Always try to use WPA2 as it implements the full version of the security standard while WPA does not.

Pre-Shared Key (PSK)

A pre-shared key is a password shared between the server and the client that unlocks the algorithm used to encrypt the data traffic between them. Without the proper password, the client and the server cannot communicate.

Extensible Authentication Protocol (EAP)

An enhanced security framework designed to improve an existing security protocol, such as WPA-PSK or WPA2-PSK.

4.1.3 Before You Begin

- Make sure the ZyXEL utility is already installed. See the Quick Start Guide for more.

4.2 ZyXEL Utility Screen Summary

This section describes the ZyXEL utility screens.

Figure 28 ZyXEL Utility Menu Summary

The following table describes the menus.

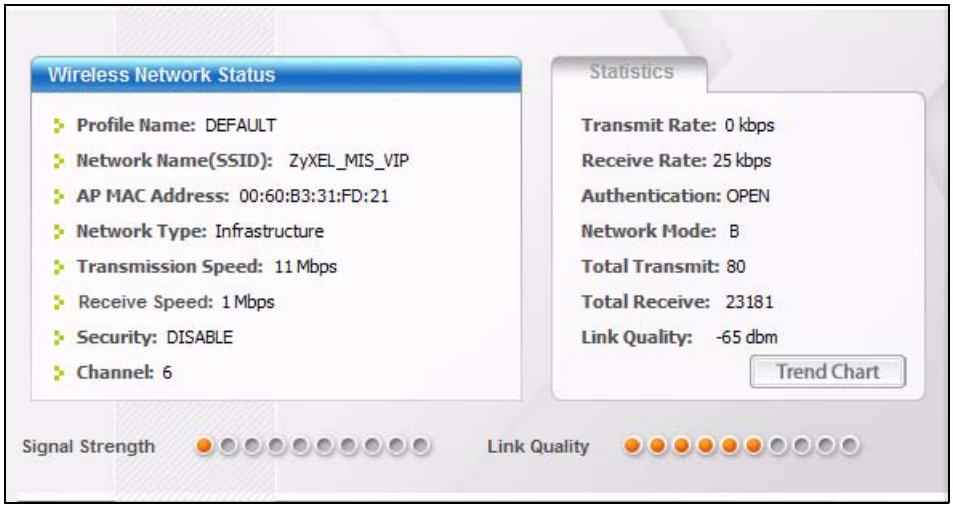
Table 4 ZyXEL Utility Menu Summary

TAB	DESCRIPTION
Link Info	Use this screen to see your current connection status, configuration and data rate statistics.
Site Survey	Use this screen to: • scan for a wireless network. • configure wireless security (if activated on the selected network). • connect to a wireless network.
Profile	Use this screen to add, delete, edit or activate a profile with a set of wireless and security settings.
Adapter	Use this screen to configure preamble type, enable power saving and use WiFi Protected Setup (WPS).

4.3 The Link Info Screen

When the ZyXEL utility starts, the **Link Info** screen displays, showing the current configuration and connection status of your NWD2105.

Figure 29 Link Info



The following table describes the labels in this screen.

Table 5 Link Info

LABEL	DESCRIPTION
Wireless Network Status	
Profile Name	This is the name of the profile you are currently using.

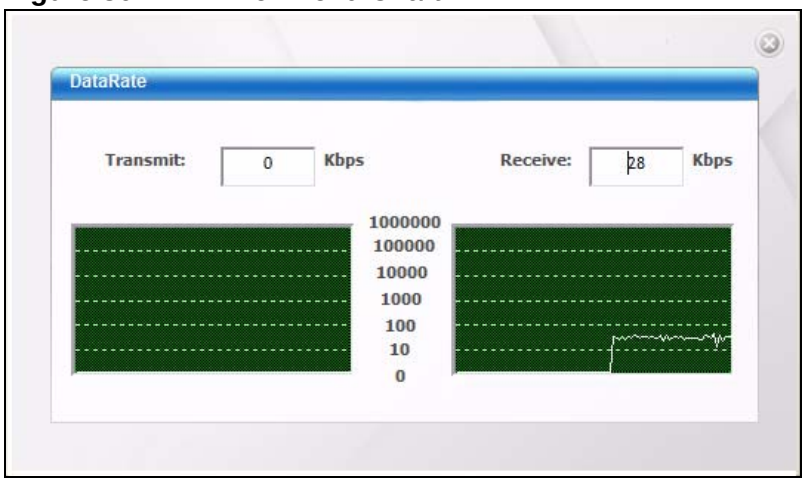
Table 5 Link Info (continued)

LABEL	DESCRIPTION
Network Name (SSID)	The SSID identifies the wireless network to which a wireless station is associated. This field displays the name of the wireless device to which the NWD2105 is associated.
AP MAC Address	This field displays the MAC address of the AP or peer computer to which the NWD2105 is associated.
Network Type	This field displays the network type (**Infrastructure** or **Ad-Hoc**) of the wireless network.
Transmission Speed	This field displays the current transmission speed of the NWD2105 in megabits per second (Mbps).
Receive Speed	This field displays the current receive speed of the NWD2105 in megabits per second (Mbps).
Security	This field displays whether data encryption is activated (**WEP** / **802.1x** / **WPA** /**WPA-PSK** / **WPA2** / **WPA2-PSK**) or inactive (**DISABLE**).
Channel	This field displays the radio channel the NWD2105 is currently using.
Statistics	
Transmit Rate	This field displays the current data transmission rate in kilobits per second (Kbps).
Receive Rate	This field displays the current data receiving rate in kilobits per second (Kbps).
Authentication	This field displays the authentication method of the NWD2105.
Network Mode	This field displays the wireless standard used by the selected wireless device. It shows **B** for 802.11b, **G** for 802.11g or **N** for 802.11n.
Total Transmit	This field displays the total number of data frames transmitted.
Total Receive	This field displays the total number of data frames received.
Link Quality	This field displays the signal strength of the NWD2105.
Trend Chart	Click this button to display the real-time statistics of the data rate in kilobits per second (Kbps).
Signal Strength	The status bar shows the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between your NWD2105 and the AP or peer computer.
Link Quality	The status bar shows the quality of wireless connection. This refers to the percentage of packets transmitted successfully. If there are too many wireless stations in a wireless network, collisions may occur which could result in a loss of messages even though you have high signal strength.

4.3.1 Trend Chart

Click **Trend Chart** in the **Link Info** screen to display a screen as shown below. Use this screen to view real-time data traffic statistics.

Figure 30 Link Info: Trend Chart



The following table describes the labels in this screen.

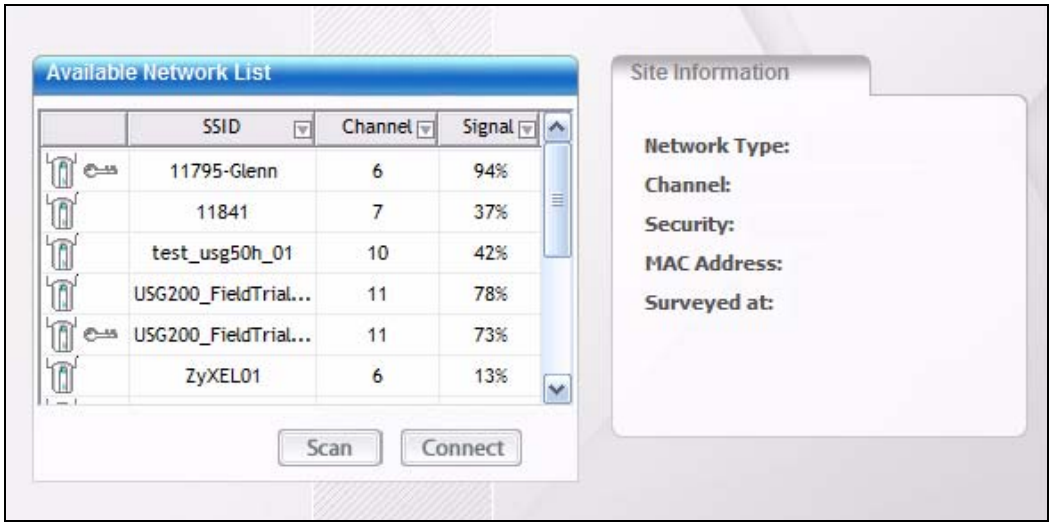
Table 6 Link Info: Trend Chart

LABEL	DESCRIPTION
Transmit	This field displays the current data transmission rate in kilobits per second (Kbps).
Receive	This field displays the current data reception rate in kilobits per second (Kbps).

4.4 The Site Survey Screen

Use the **Site Survey** screen to scan for and connect to a wireless network automatically.

Figure 31 Site Survey



The following table describes the labels in this screen.

Table 7 Site Survey

LABEL	DESCRIPTION
Available Network List	Click a column heading to sort the entries.
, , or	denotes that the wireless device is in infrastructure mode and the wireless security is activated. denotes that the wireless device is in infrastructure mode but the wireless security is deactivated. denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated. denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated.
SSID	This field displays the SSID (Service Set IDentifier) of each wireless device.
Channel	This field displays the channel number used by each wireless device.
Signal	This field displays the signal strength of each wireless device.
Scan	Click **Scan** to search for available wireless devices within transmission range.
Connect	Click **Connect** to associate to the selected wireless device.
Site Information	Click an entry in the **Available Network List** table to display the information of the selected wireless device.

Table 7 Site Survey (continued)

LABEL	DESCRIPTION
Network Type	This field displays the network type (**Infrastructure** or **Ad Hoc**) of the wireless device.
Channel	This field displays the channel number used by each wireless device.
Security	This field shows whether data encryption is activated (**WEP**, **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK** or **802.1x**) or inactive (**DISABLE**).
MAC address	This field displays the MAC address of the wireless device.
Surveyed at	This field displays the time when the wireless device was scanned.

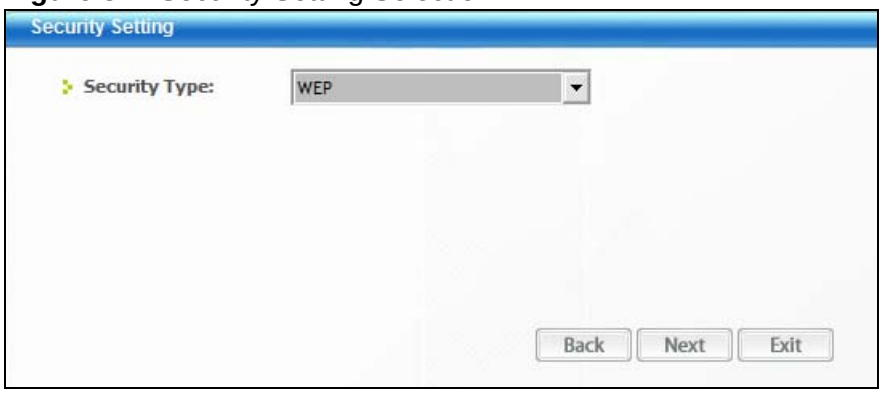
4.4.1 Security Settings

When you configure the NWD2105 to connect to a network with wireless security activated and the security settings are disabled on the NWD2105, the screen varies according to the encryption method used by the selected network.

4.4.1.1 Security Type Selection

When you choose to connect to a network that has security, you are presented with is a security selection screen. Choose the security of the network you are attempting to join.

Figure 32 Security Setting Selection



The following table describes the labels in this screen.

Table 8 Security Setting: WEP

LABEL	DESCRIPTION
Security Type	Select the security type that matches the security setting of the network you're trying to join. The options are: **WEP**, **WPA**, **WPA2**, **WPA-PSK**, **WPA2-PSK**, and **802.1x**.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.

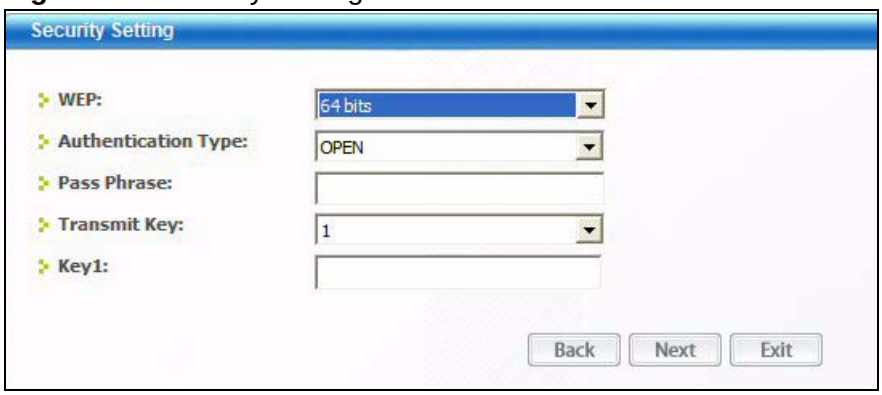
Table 8 Security Setting: WEP (continued)

LABEL	DESCRIPTION
Next	Click **Next** to confirm your selections and advance to the **Security Settings** screen that corresponds to the one you select here.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.4.1.2 WEP Encryption

Configure WEP security in this screen.

Figure 33 Security Setting: WEP



The following table describes the labels in this screen.

Table 9 Security Setting: WEP

LABEL	DESCRIPTION
Security Settings	
WEP	Select **64 Bits** or **128 Bits** to activate WEP encryption and then fill in the related fields.
Authentication Type	Select an authentication method. Choices are **Open** and **Shared**. Refer to Section 3.3.1.1.2 on page 40 for more information.
Pass Phrase	Enter a passphrase of up to 32 case-sensitive printable characters. As you enter the passphrase, the NWD2105 automatically generates four different WEP keys and displays the first in the key field below. Refer to Section 3.3.1.1.1 on page 39 for more information.
Transmit Key	Select a default WEP key to use for data encryption. The key displays in the adjacent field.

Table 9 Security Setting: WEP (continued)

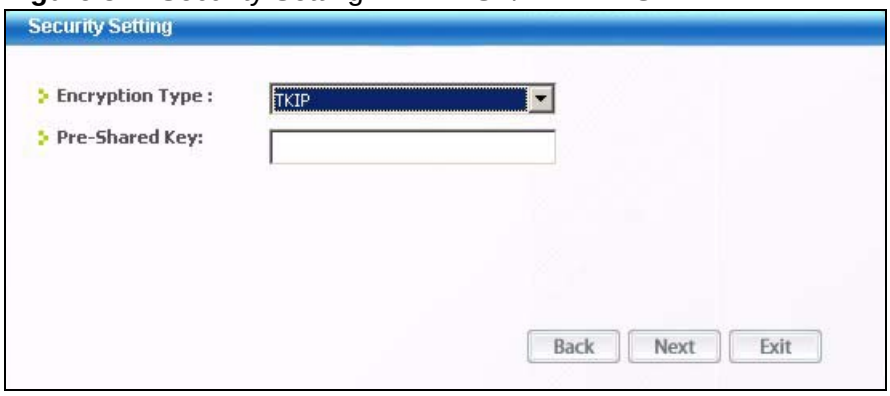
LABEL	DESCRIPTION
Key x (where x is a number between 1 and 4)	Select this option if you want to manually enter the WEP keys. Enter the WEP key in the field provided. If you select **64 Bits** in the **WEP** field. Enter either 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 11AA22BB33) for HEX key type. or Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for ASCII key type. If you select **128 Bits** in the **WEP** field, Enter either 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 00112233445566778899AABBCC) for HEX key type or Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for ASCII key type. Note: The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN. ASCII WEP keys are case sensitive.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the **Summary** screen. Refer to Section 4.4.2 on page 61.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.4.1.3 WPA-PSK/WPA2-PSK

Configure WPA-PSK/WPA2-PSK security in this screen.

Note: The procedure to configure WPA or WPA2 is different in Windows Vista. See Section 4.7 on page 71 for information on setting up your NWD2105 to use WPA or WPA2 in Vista.

Figure 34 Security Setting: WPA-PSK/WPA2-PSK



The following table describes the labels in this screen.

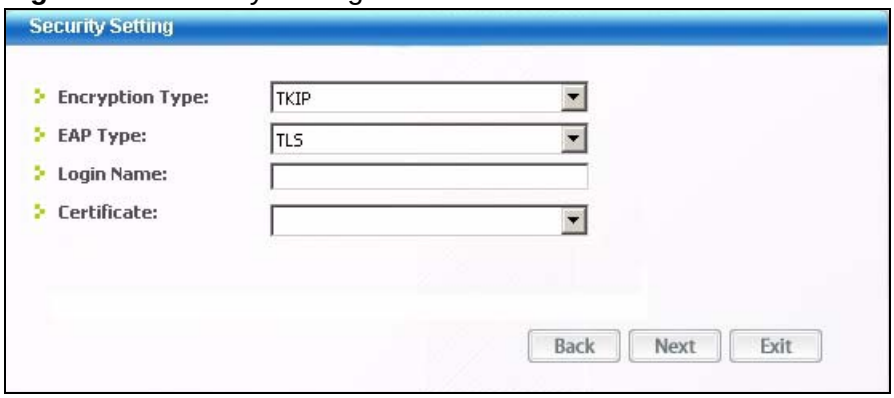
Table 10 Security Setting: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Encryption Type	The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials. Select the encryption type (**TKIP** or **AES**) for data encryption. Refer to Section 3.3.1.3 on page 41 for more information.
Pre-Shared Key	Type a pre-shared key (same as the AP or peer device) of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the **Summary** screen. Refer to Section 4.4.2 on page 61.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.4.1.4 WPA/WPA2

The screen that displays when you select **WPA** or **WPA2** differs, depending on the **EAP Type** you select (**TLS**, **PEAP** or **TTLS**).

Figure 35 Security Settings: WPA/WPA2



The following table describes the labels in this screen.

Table 11 Security Setting: WPA/WPA2

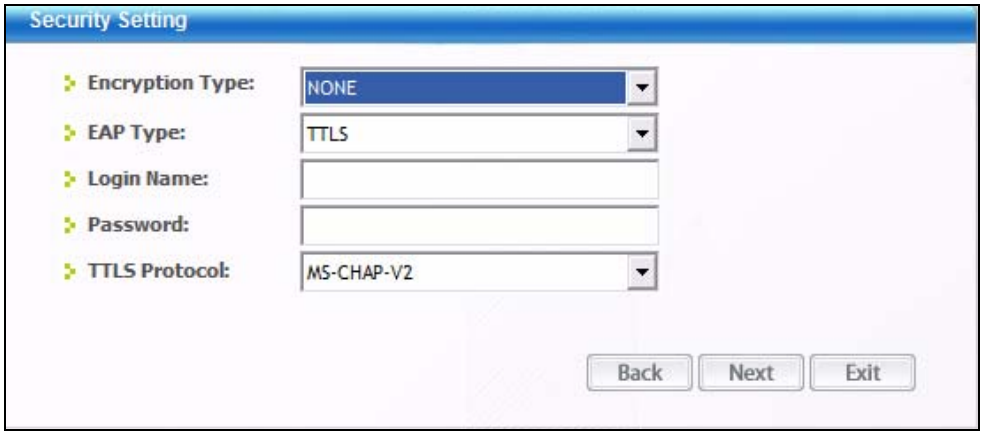
LABEL	DESCRIPTION
Encryption Type	The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials. Select the encryption type (**TKIP** or **AES**) for data encryption. Refer to Section 3.3.1.3 on page 41 for more information.
EAP Type	The type of authentication you use depends on the RADIUS server or AP. Select an authentication method from the drop down list. Options are **TLS**, **PEAP** and **TTLS** (at the time of writing, TTLS is not available in Windows Vista).
Login Name	Enter a user name. This is the user name that you or an administrator set up on a RADIUS server.
Password	This field is not available when you select **TLS** in the **EAP Type** field. Enter the password associated with the user name above.
Certificate	This field is only available when you select **TLS** in the **EAP Type** field. Click **Browse** to select a certificate. Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.
PEAP Inner EAP	This field is only available when you select **PEAP** in the **EAP Type** field. The PEAP method used by the RADIUS server or AP for client authentication is **MS CHAP v2**.
TTLS Protocol	This field is available only when you select **TTLS** in the **EAP Type** field. Select a TTLS protocol that the RADIUS server uses. Options are **CHAP**, **MS-CHAP**, **MS-CHAP-V2** and **PAP**. Note: This feature is not available on Windows Vista.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the **Summary** screen. Refer to Section 4.4.2 on page 61.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.4.1.5 IEEE 802.1x

Configure IEEE 802.1x security with various authentication methods in this screen.

Note: The procedure to configure 802.1x is different in Windows Vista. See Section 4.7 on page 71 for information on setting up your NWD2105 to use 802.1x in Vista.

Figure 36 Security Setting: 802.1x



The following table describes the labels in this screen.

Table 12 Security Settings: IEEE 802.1x

LABEL	DESCRIPTION
Encryption Type	Select **WEP** if the access point is configured to use 802.1x with WEP encryption. A dynamic WEP key is generated automatically. Otherwise, select **NONE** (at the time of writing, this is not available in Windows Vista).
EAP Type	The type of authentication you use depends on the RADIUS server or AP. Select an authentication method from the drop down list. Options are **TLS**, **PEAP** and **TTLS** (at the time of writing, TTLS is not available in Windows Vista).
Login Name	Enter a user name. This is the user name that you or an administrator set up on a RADIUS server.
Password	This field is not available when you select **TLS** in the **EAP Type** field. Enter the password associated with the user name above.
Certificate	This field is only available when you select **TLS** in the **EAP Type** field. Click **Browse** to select a certificate. Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.

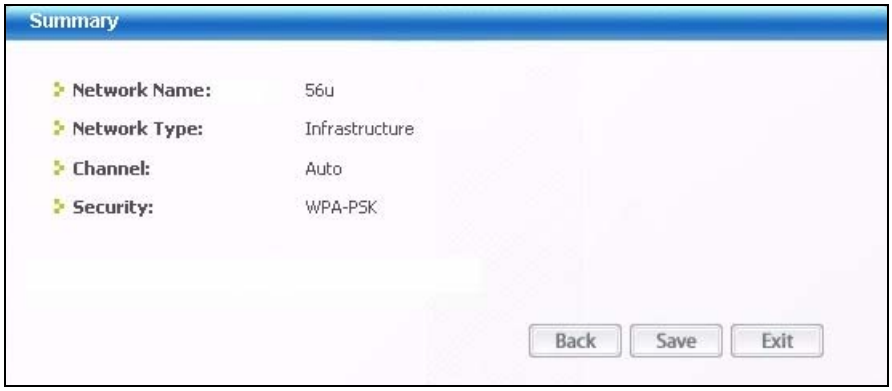
Table 12 Security Settings: IEEE 802.1x

LABEL	DESCRIPTION
TTLS Protocol	This field is available only when you select **TTLS** in the **EAP Type** field. Select a TTLS protocol that the RADIUS server uses. Options are **CHAP**, **MS-CHAP**, **MS-CHAP-V2** and **PAP**. Note: This feature is not available on Windows Vista.
PEAP Inner EAP	This field is only available when you select **PEAP** in the **EAP Type** field. The PEAP method used by the RADIUS server or AP for client authentication is **MS CHAP v2**.
Validate Server Certificate (Click to Enable)	Select this option to validate a server's certificate when you select **PEAP** in the **EAP Type** field.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the **Summary** screen. Refer to Section 4.4.2 on page 61.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.4.2 Summary Screen

Use this screen to confirm and save the security settings.

Figure 37 Summary Screen



The following table describes the labels in this screen.

Table 13 Summary Screen

LABEL	DESCRIPTION
Network Name (SSID)	This field displays the SSID previously entered.
Network Type	This field displays the network type (**Infrastructure** or **Ad-Hoc**) of the wireless device.
Channel	This field displays the channel number used by the profile.

Table 13 Summary Screen

LABEL	DESCRIPTION
Security	This field shows whether data encryption is activated (**WEP**, **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK**, **802.1x**) or inactive (**DISABLE**).
Back	Click **Back** to return to the previous screen.
Save	Click **Save** to save the changes back to the NWD2105 and display the **Link Info** screen.
Exit	Click **Exit** to discard changes and return to the **Site Survey** screen.

4.5 The Profile Screen

A profile is a set of wireless parameters that you need to connect to a wireless network. With a profile activated, each time you start the NWD2105, it automatically scans for the specific SSID and joins that network with the pre-defined wireless security settings. If the specified network is not available, the NWD2105 cannot connect to a network.

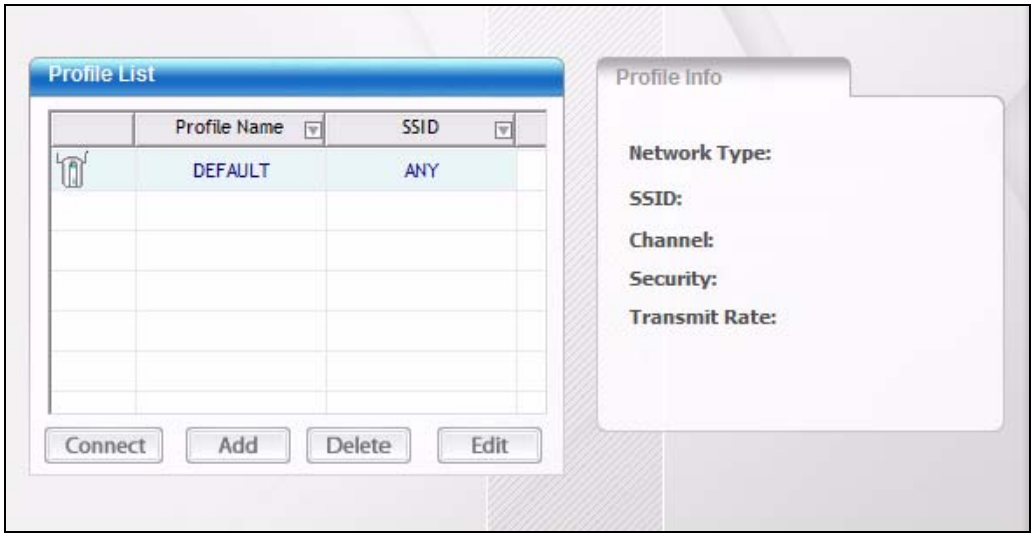
If you do not configure and activate a profile, each time you start the NWD2105, the NWD2105 uses the default profile to connect to any available network that has no security enabled.

The default profile is a profile that allows you to connect to any SSID that has no security enabled.

Click the **Profile** tab in the ZyXEL utility program to display the **Profile** screen as shown next.

The profile function allows you to save the wireless network settings in this screen, or use one of the pre-configured network profiles.

Figure 38 Profile



The following table describes the labels in this screen.

Table 14 Profile

LABEL	DESCRIPTION
Profile List	Click a column heading to sort the entries.
, , or	denotes that the wireless device is in infrastructure mode and the wireless security is activated. denotes that the wireless device is in infrastructure mode but the wireless security is deactivated. denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated. denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated.
Profile Name	This is the name of the pre-configured profile.
SSID	This is the SSID of the wireless network to which the selected profile associate.
Connect	To use and activate a previously saved network profile, select a pre-configured profile name in the table and click **Connect**.
Add	To add a new profile into the table, click **Add**.
Delete	To delete an existing wireless network configuration, select a profile in the table and click **Delete**.
Edit	To edit an existing wireless network configuration, select a profile in the table and click **Edit**.
Profile Info	The following fields display detailed information of the selected profile in the **Profile List** table.
Network Type	This field displays the network type (**Infrastructure** or **Ad-Hoc**) of the profile.

Table 14 Profile (continued)

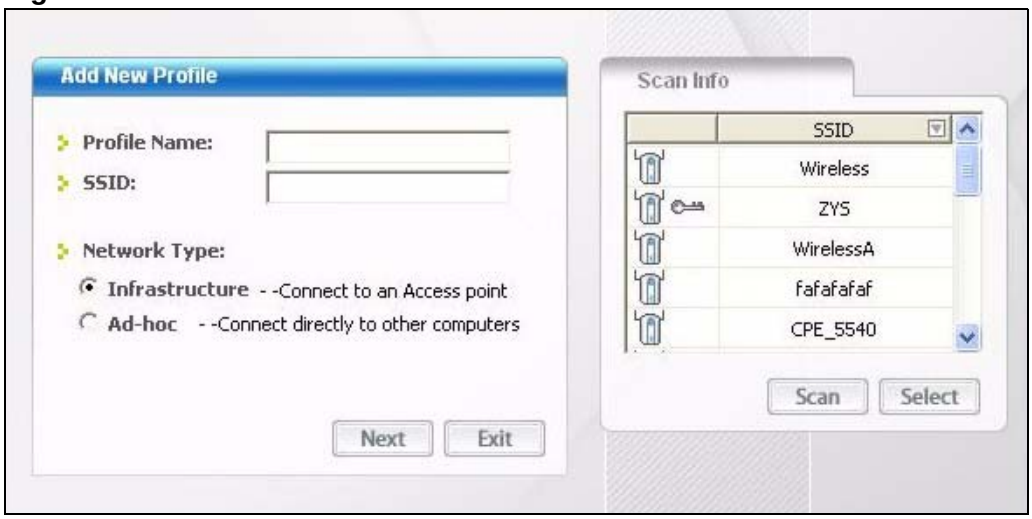
LABEL	DESCRIPTION
SSID	This field displays the network's Service Set IDentity (the name of the network).
Channel	This field displays the channel number used by the profile.
Security	This field shows whether data encryption is activated (**WEP**, **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK** or **802.1x**) or inactive (**DISABLE**).
Transmit Rate	This field displays the transmission speed of the selected profile in megabits per second (Mbps).

4.5.1 Adding a New Profile

Follow the steps below to add a new profile.

1 Click **Add** in the **Profile** screen. An **Add New Profile** screen displays as shown next.

Figure 39 Profile: Add a New Profile



The following table describes the labels in this screen.

Table 15 Profile: Add a New Profile

LABEL	DESCRIPTION
Add New Profile	
Profile Name	Enter a descriptive name in this field.
SSID	Select an available wireless device in the **Scan Info** table and click **Select**, or enter the SSID of the wireless device to which you want to associate in this field manually. Otherwise, enter **Any** to have the NWD2105 associate to any AP or roam between any infrastructure wireless networks.
Network Type	Select **Infrastructure** to associate to an AP. Select **Ad-Hoc** to associate to a peer computer.
Next	Click **Next** to go to the next screen.

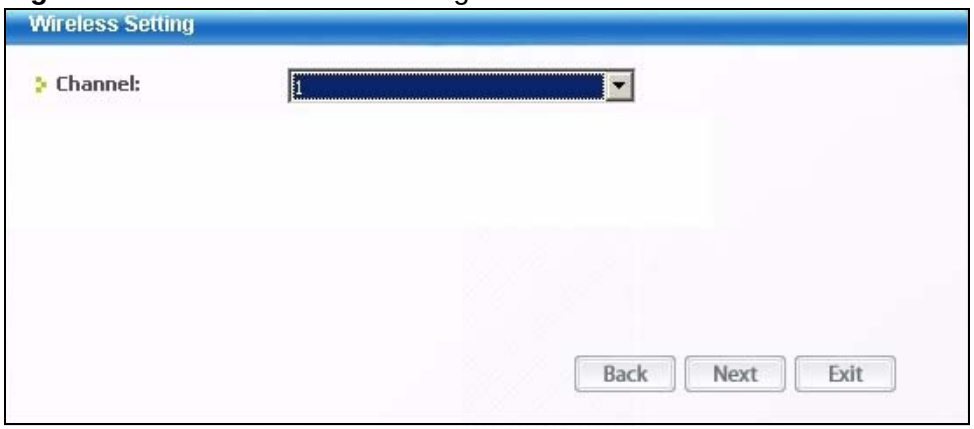
Table 15 Profile: Add a New Profile (continued)

LABEL	DESCRIPTION
Exit	Click **Exit** to go back to the previous screen without saving.
Scan Info	This table displays the information of the available wireless networks within the transmission range.
, , or	denotes that the wireless device is in infrastructure mode and the wireless security is activated. denotes that the wireless device is in infrastructure mode but the wireless security is deactivated. denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated. denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated.
SSID	This field displays the SSID (Service Set IDentifier) of each AP or peer device.
Scan	Click **Scan** to search for available wireless devices within transmission range.
Select	Select an available wireless device in the table and click **Select** to add it to this profile. Whenever you activate this profile, the NWD2105 associates to the selected wireless network only.

2 If you select the **Infrastructure** network type in the previous screen, skip to step 3. If you select the **Ad-Hoc** network type in the previous screen, a screen displays as follows. Select a **Channel** number and **Wireless Mode** and click **Next** to continue.

Note: To associate to an ad-hoc network, you must use the same channel as the peer computer.

Figure 40 Profile: Wireless Settings



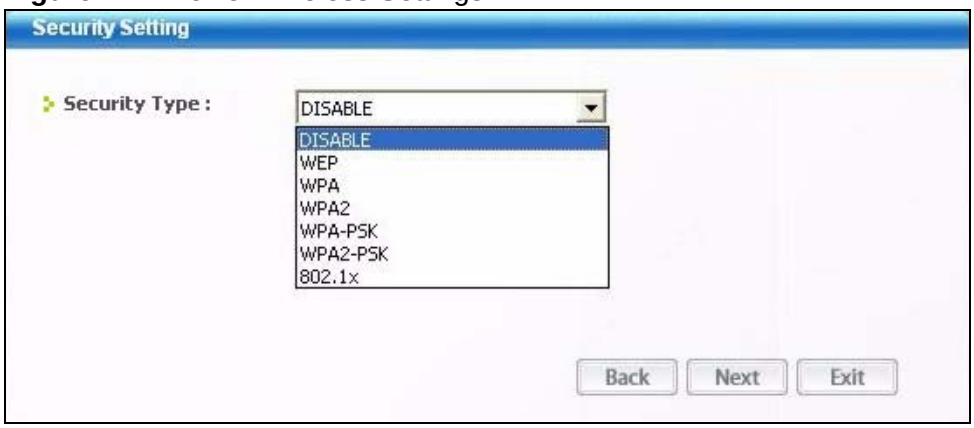
The following table describes the labels in this screen.

Table 16 Profile: Wireless Settings

LABEL	DESCRIPTION
Wireless Settings	
Channel	Select a channel number from the drop-down list box. To associate to an ad-hoc network, you must use the same channel as the peer computer.

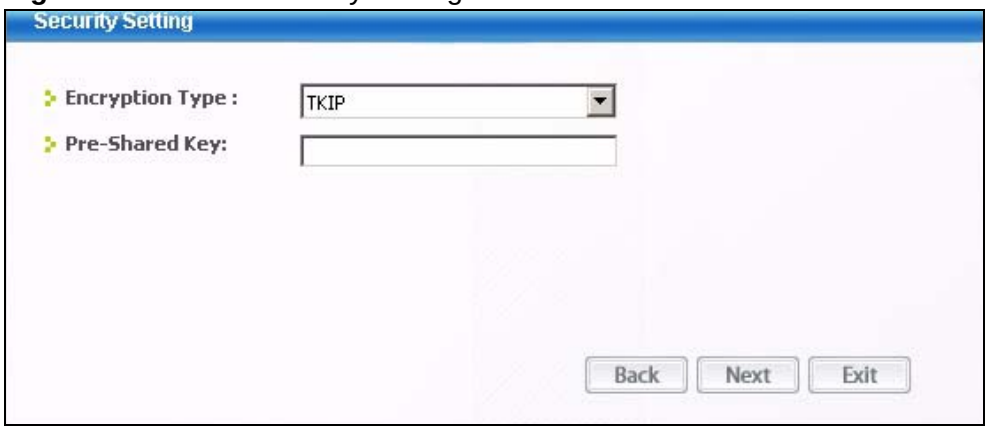
3 If you selected **Infrastructure** network type in the first screen, select **WEP**, **WPA**, **WPA2**, **WPA-PSK**, **WPA2-PSK** or **802.1x** from the drop-down list box to enable data encryption. If you selected **Ad-Hoc** network type in the first screen, you can use only **WEP** encryption method. Otherwise, select **DISABLE** to allow the NWD2105 to communicate with the access points or other peer wireless computers without any data encryption, and skip to step 5.

Figure 41 Profile: Wireless Settings



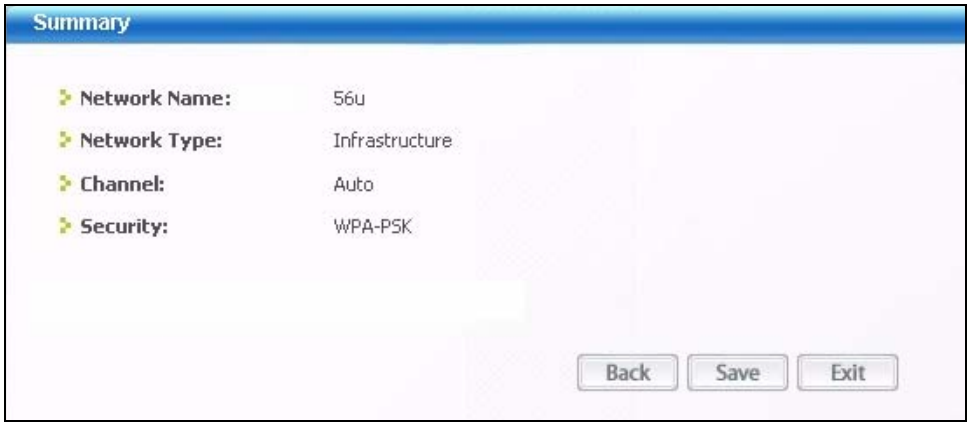
4 The screen varies depending on the encryption method you select in the previous screen. The settings must be exactly the same on the AP or other peer wireless computers as they are on the NWD2105. Refer to Section 5.4.1 on page 80 for detailed information on wireless security configuration.

Figure 42 Profile: Security Settings



5 This read-only screen shows a summary of the new profile settings. Verify that the settings are correct. Click **Save** to save and go to the next screen. Click **Back** to return to the previous screen. Otherwise, click **Exit** to go back to the **Profile** screen without saving.

Figure 43 Profile: Confirm New Settings



6 To use this network profile, click the **Activate Now** button. Otherwise, click the **Activate Later** button. You can activate only one profile at a time.

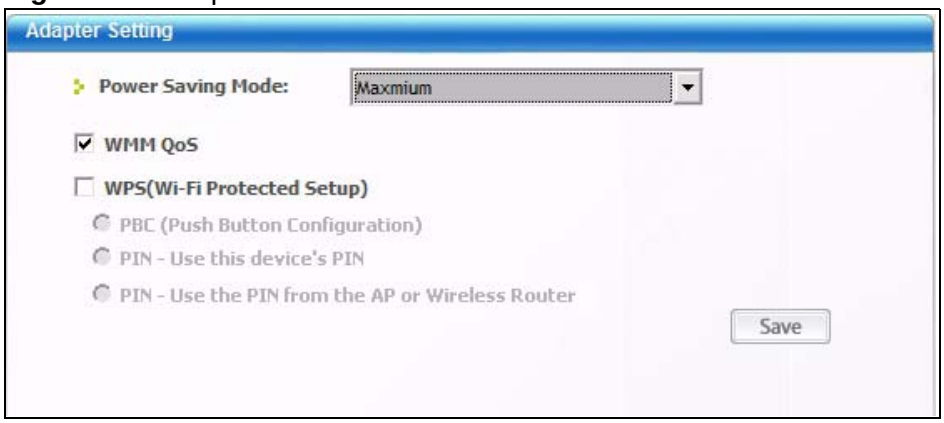
Note: Once you activate a profile, the ZyXEL utility will use that profile the next time it is started.

Figure 44 Profile: Activate the Profile

4.6 The Adapter Screen

To set the other advanced features on the NWD2105, click the **Adapter** tab.

Figure 45 Adapter



The following table describes the labels in this screen.

Table 17 Adapter

LABEL	DESCRIPTION
Adapter Setting	
Power Saving Mode	Select **Maximum** or **Normal** to save power. This forces the NWD2105 to go to sleep mode when it is not transmitting data. When you select **Off**, the NWD2105 will never go to sleep mode. At the time of writing, this field is not available in Windows Vista.
WMM QoS	Select this to enable Wi-fi MultiMedia Quality of Service on the NWD2105. At the time of writing, this field is not available in Windows Vista.
WPS (WiFi Protected Setup)	Select this to enable Wi-fi Protected Setup on the NWD2105.
PBC (Push Button Configuration)	Select this to use the PBC (Push-Button Configuration) WPS mode. When you use the PBC mode you do not use a PIN. When you select this, the **PBC (Push Button Configuration** screen appears (see Section 4.6.1 on page 69).
PIN - Use This Device's PIN	Select this to use the PIN (Personal Identification Number) WPS mode. Use this option when you want to enter the NWD2105's PIN in another WPS-enabled device. When you select this, the **PIN - Use this Device's PIN** screen appears (see Section 4.6.2 on page 69).

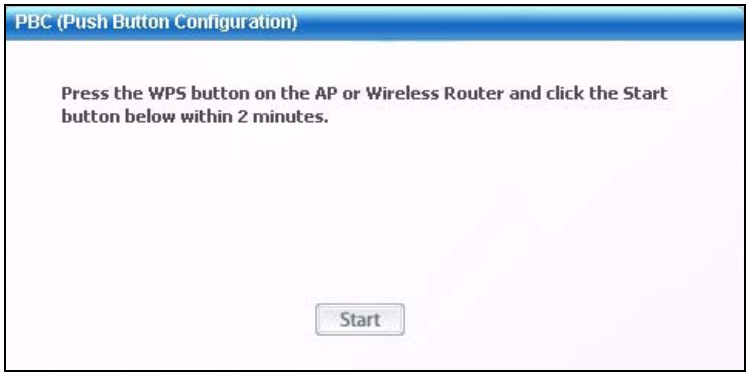
Table 17 Adapter (continued)

LABEL	DESCRIPTION
PIN - Use the PIN From the AP or Wireless Router	Select this to use the PIN (Personal Identification Number) WPS mode. Use this option when you want to enter the PIN from another WPS-enabled device in the NWD2105. When you select this, the **PIN - Use the PIN From the AP or Wireless Router** screen appears (see Section 4.6.3 on page 70).
Save	Click **Save** to save the changes to the NWD2105 and return to the **Link Info** screen.

4.6.1 WPS: PBC (Push Button Configuration)

This screen allows you to use the WPS Push Button Configuration mode. See Section 3.4.1 on page 42 for more information. Select **WPS** and **PBC (Push Button Configuration)** in the **Adapter** screen. The following screen displays.

Figure 46 WPS: PBC (Push Button Configuration)


PBC (Push Button Configuration)
Press the WPS button on the AP or Wireless Router and click the Start button below within 2 minutes.
Start

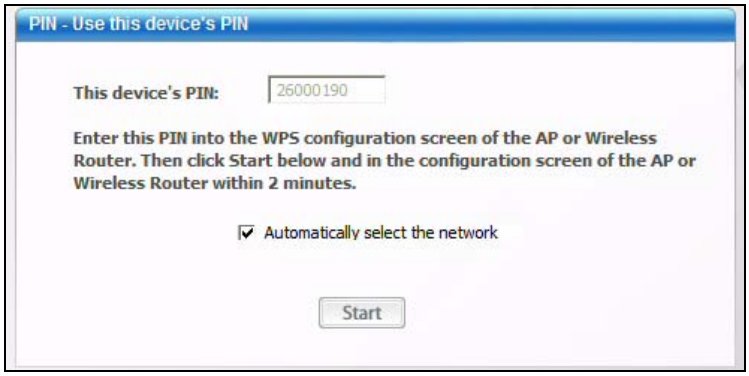
Press **Start** when you want to begin the WPS process. You must also press the button on the other device within two minutes.

4.6.2 WPS: PIN - Use this Device's PIN

This screen allows you to use the WPS Personal Identification Number mode, by entering the NWD2105's unique PIN in the configuration utility of the other WPS-enabled device. See Section 3.4.2 on page 42 for more information. Select **WPS**

and **PIN - Use this Device's PIN** in the **Adapter** screen. The following screen displays.

Figure 47 WPS: PIN - Use this Device's PIN


PIN - Use this device's PIN
This device's PIN:
26000190
Enter this PIN into the WPS configuration screen of the AP or Wireless Router. Then click Start below and in the configuration screen of the AP or Wireless Router within 2 minutes.
Automatically select the network
Start

The following table describes the labels in this screen.

Table 18 WPS: PIN - Use this Device's PIN

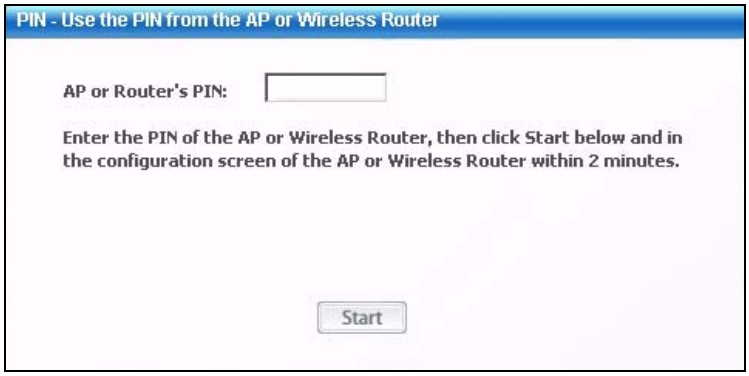
LABEL	DESCRIPTION
This device's PIN	This is the NWD2105's Personal Identification Number (PIN). This field is read-only. Enter the number that displays in this field into the configuration interface of the other WPS-enabled device. Note: Each time this screen displays, the PIN is different. The PIN is valid for only one WPS transaction.
Start	Click this to start WPS. You must start WPS on the other WPS-enabled device within two minutes.

4.6.3 WPS: PIN - Use the PIN from the AP or Wireless Router

This screen allows you to use the WPS Personal Identification Number mode, by entering the PIN from another WPS-enabled device into the NWD2105's utility. See Section 3.4.2 on page 42 for more information. Select **WPS** and **PIN - Use**

the PIN from the AP or Wireless Router in the **Adapter** screen. The following screen displays.

Figure 48 WPS: PIN - Use the PIN from the AP or Wireless Router


PIN - Use the PIN from the AP or Wireless Router
AP or Router's PIN:
Enter the PIN of the AP or Wireless Router, then click Start below and in the configuration screen of the AP or Wireless Router within 2 minutes.
Start

The following table describes the labels in this screen.

Table 19 WPS: PIN - Use the PIN from the AP or Wireless Router

LABEL	DESCRIPTION
AP or Router's PIN	Enter the PIN from your AP or wireless router in this field before you click **Start**.
Start	Click this to start WPS. You must start WPS on the other WPS-enabled device within two minutes.

4.7 Security Settings in Windows Vista

When you use the NWD2105 in Windows Vista, the procedure for setting up WPA, WPA2 and 802.1x security settings is different from that of other operating systems (other security types are not affected).

The procedures for setting up WPA, WPA2 or 802.1x in Vista are the same. However, the procedure differs depending on whether you use PEAP (Protected Extensible Authentication Protocol) or TLS (Transport Layer Security) encryption. Consult your network administrator if you are unsure which type of encryption to use.

See Section 4.7.1 on page 72 to use PEAP, or see Section 4.7.2 on page 73 to use TLS.

Note: TTLS (Tunneled TLS) is not available when using Windows Vista, at the time of writing.

4.7.1 Using PEAP in Vista

Take the following steps to set up WPA, WPA2 or 802.1x security using PEAP in Windows Vista.

1 Either select the AP to which you want to connect in the **Site Survey** screen (see Section 4.4 on page 54), or configure a profile in the normal way (see Section 4.5 on page 62).

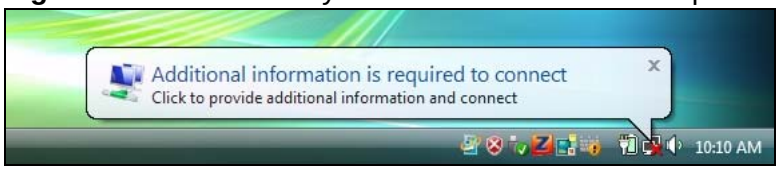
2 In the **WPA**, **WPA2** or **802.1x** security screen (see Section 4.4.1.4 on page 58 and Section 4.4.1.5 on page 59), select **PEAP** as the **EAP Type**. Note that the **Login Name** and **Password** fields are greyed-out (not available).

3 Click **Next**.

4 In the **Summary** screen that appears, click **Save**.

5 A message similar to the following appears in the bottom-right of your screen. Click the message.

Figure 49 Vista Security: Additional Information Required



6 The **Enter Credentials** screen displays. Enter your **User name** and **Password** for the network to which you want to connect.

Figure 50 Vista Security: Enter Credentials

Note: If you are not sure what to enter, contact your network administrator.

7 Click **OK**. The **Enter Credentials** screen disappears and the NWD2105 tries to connect to the network. The ZyXEL utility's **Link Info** screen displays, showing the connection status (see Section 4.3 on page 51). If the **Link Info** screen displays an active connection, you have successfully completed the procedure.

4.7.2 Using TLS in Vista

Take the following steps to set up WPA, WPA2 or 802.1x security using TLS in Windows Vista.

1 Either select the AP to which you want to connect in the **Site Survey** screen (see Section 4.4 on page 54), or configure a profile (see Section 4.5 on page 62) in the normal way.

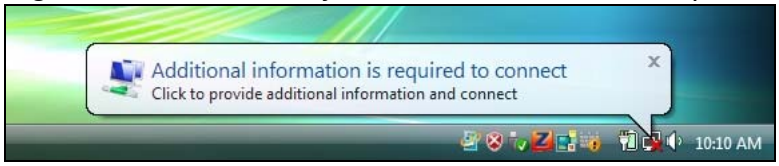
2 In the **WPA**, **WPA2** or **802.1x** security screen, select **TLS** as the **EAP Type**. Note that the **Login Name**, **Certificate** and **Validate Server Certificate** fields are greyed-out (not available).

3 Click **Next**.

4 In the **Summary** screen, click **Save**.

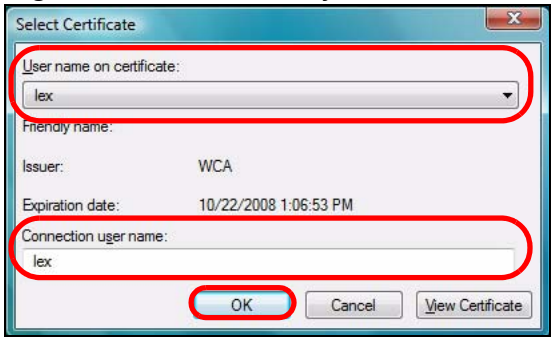
5 A message similar to the following appears in the bottom-right of your screen. Click the message.

Figure 51 Vista Security: Additional Information Required



6 The **Select Certificate** screen displays. Select the certificate you want to use in order to authenticate with the server, and enter your username.

Figure 52 Vista Security: Select Certificate



Note: If you do not have the right certificate, or are not sure which certificate you should use, contact your network administrator.

7 Click **OK**. The **Select Certificate** screen disappears and the NWD2105 tries to connect to the network. The ZyXEL utility's **Link Info** screen displays, showing the connection status (see Section 4.3 on page 51). If the **Link Info** screen displays an active connection, you have successfully completed the procedure.

5

AP Mode

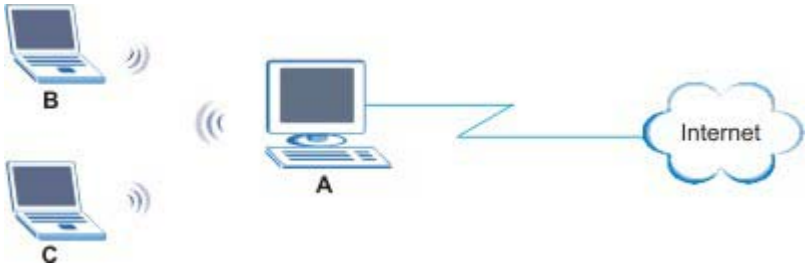
5.1 Overview

This section shows you how to configure your NWD2105 in **AP Mode** using the Windows version of the ZyXEL Utility.

Note: Some features available in Windows XP or Windows 2000 are not available in Windows Vista.

AP Mode allows you to set up a wireless network without using a pre-existing AP. The following figure shows a sample AP network set up.

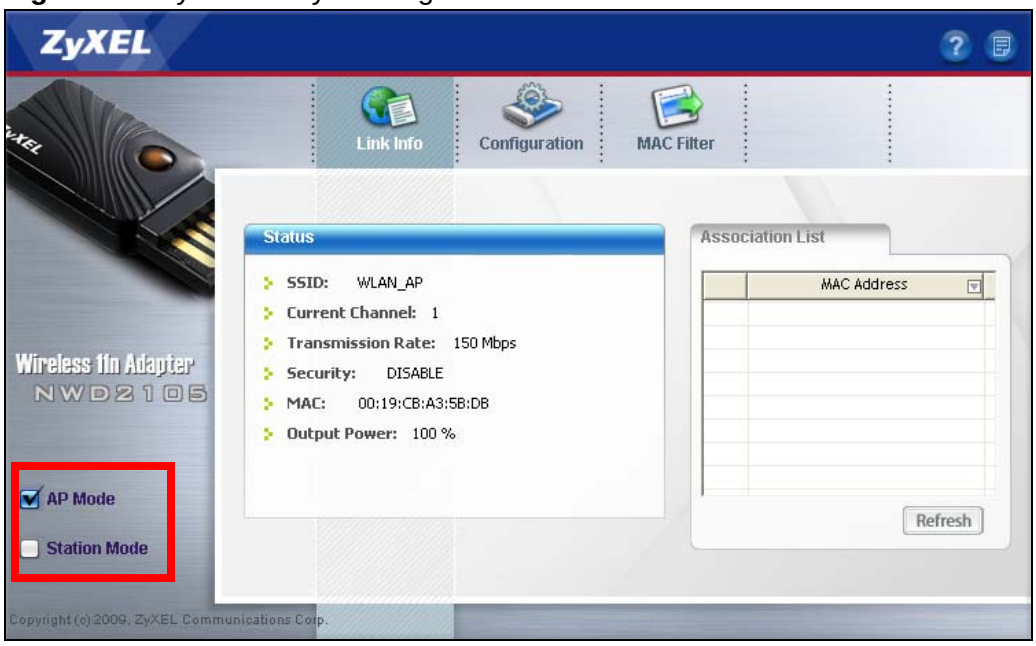
Figure 53 AP Network Example .



Here, the NWD2105 is installed on computer **A** and set to operate in access point mode. Computer **A** provides an Internet connection to the wireless LAN, so wireless stations **B** and **C** can access the Internet.

Select the **AP Mode** option the ZyXEL Utility to have the device function as an access point.

Figure 54 ZyXEL Utility: Setting AP Mode .



5.1.1 What You Can Do in This Section

- On the **Link Info** screen, you can see your AP's current transmission and security status See Section 5.3 on page 78 for details.
- On the **Configuration** screen, you can set up the broadcast parameters for your access point as well as its security options. See Section 5.4 on page 79 for details.
- On the **MAC Filter** screen, you can configure the NWD2105 to give exclusive access to devices or exclude specific devices from connecting to the AP. See Section 5.5 on page 83 for details.

5.1.2 What You Need to Know

The following terms and concepts may help as you read through this section.

MAC Address

On a local area network (LAN) or other network, the MAC address is a computer's unique hardware number. On an Ethernet LAN, it's the same as your Ethernet address. The MAC layer frames data for transmission over the network, then passes the frame to the physical layer interface where it is transmitted as a stream of bits.

See Also...

The terms and concepts introduced in Chapter 4 on page 49 apply to this chapter as well.

5.1.3 Before You Begin

Make sure the ZyXEL Utility is already installed. See the Quick Start Guide for more.

To bridge your wired and wireless network using the NWD2105, the following requirements must be met:

- The NWD2105 must be installed on a computer connected to the wired network.
- Either bridge the two interfaces (wireless and wired) on the computer (using the **Configuration** screen) or configure network sharing.
- Set the wireless station's IP address to be dynamic if you want the wireless stations to access the wired network or the Internet through the NWD2105. Refer to Appendix A on page 101 for how to configure your computer's IP address.

5.2 AP Mode Screen Summary

This section describes the ZyXEL Utility screens while in **AP Mode**.

Figure 55 ZyXEL Utility Menu Summary

The following table describes the menus.

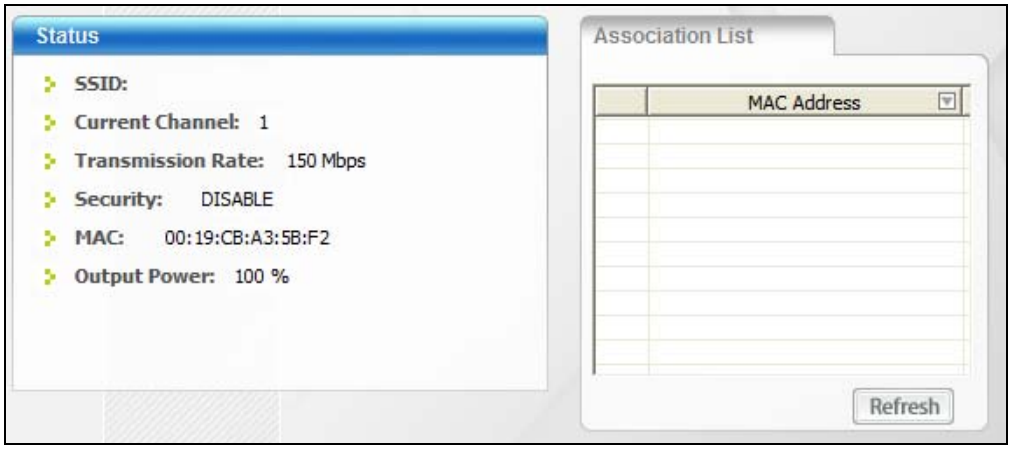
Table 20 ZyXEL Utility Menu Summary

TAB	DESCRIPTION
Link Info	Use this screen to see your current connection status, configuration and data rate statistics.
Configuration	Use this screen to configure wireless LAN settings.
MAC Filter	Use this screen to configure which computer(s) you want access to the wireless LAN through the NWD2105.

5.3 The Link Info Screen

When you enter AP Mode, the **Link Info** screen displays, showing the current configuration and connection status of your NWD2105 access point.

Figure 56 Link Info



The following table describes the labels in this screen.

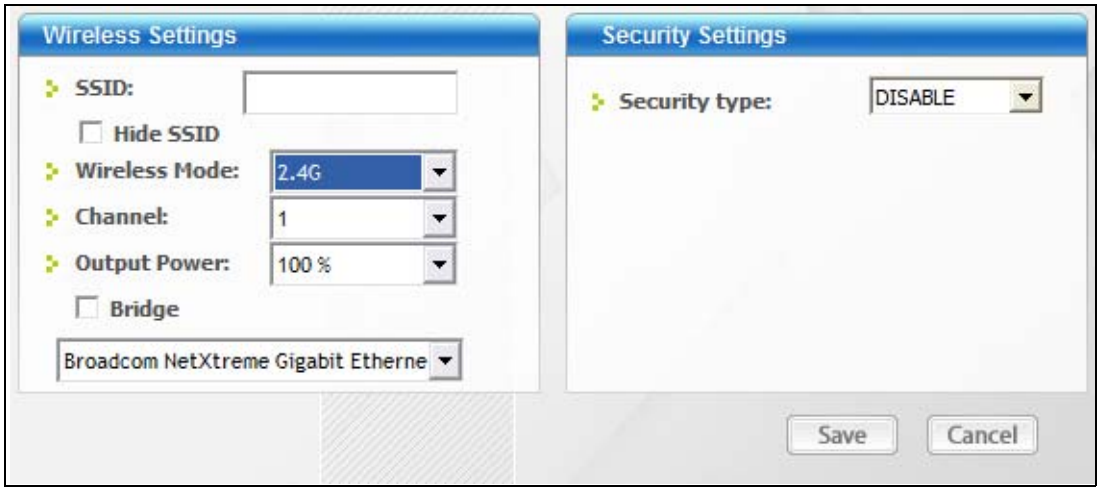
Table 21 Link Info

LABEL	DESCRIPTION
Status	
SSID	This field displays the name that identifies your NWD2105 in the wireless LAN network.
Current Channel	This field displays the radio channel the NWD2105 is currently using.
Transmission Rate	This field displays the current transmission rate of the NWD2105 in megabits per second (Mbps).
Security	This field shows whether data encryption is activated (**WEP**, **WPA**, **WPA2**, **WPA-PSK** or **WPA2-PSK**) or inactive (**DISABLE**).
MAC	This field displays the MAC address of the NWD2105.
Output Power	This field shows the strength of the NWD2105's antenna gain or transmission power.
Association List	This table lists the wireless clients that are currently connected to the NWD2105.
	denotes a wireless client without wireless security. denotes a wireless client with wireless security enabled.
MAC Address	This field displays the MAC addresses of a wireless client that is currently connected to the NWD2105.
Refresh	Click **Refresh** to update this screen.

5.4 The Configuration Screen

The **Configuration** screen allows you to set up the broadcast parameters for your access point as well as its security options.

Figure 57 The Configuration Screen



The following table describes the labels in this screen.

Table 22 Configuration

LABEL	DESCRIPTION
Wireless Settings	
SSID	Enter a name for your AP This name is broadcast to all wireless-capable devices in range and can be used to connect to your AP. You can enter up to 32 printable ASCII characters in this field.
Hide SSID	Select this option to keep your AP's SSID private. Only users who explicitly enter the SSID name in their connection window while connecting will be able to "see" it. While effective at deterring the casual user from inadvertantly connecting to your AP, it is the weakest of all wireless security. Anyone with a basic sniffer program will be able to detect the channel.
Wireless Mode	This displays a list of available wireless modes. As of this writing, the NWD2105 only supports 2.4 GHz.
Channel	Select a channel on which on broadcast your AP's wireless signal. If there are a high number of APs broadcast within range of one another, try to use a channel that is either not in use or that has the fewest number of broadcasters. Too many APs using the same channel can interfere with one another.

Table 22 Configuration (continued)

LABEL	DESCRIPTION
Output Power	Set this field if you need to conserve power consumption (especially for notebook computers). This control changes the strength of the NWD2105's antenna gain or transmission power. Antenna gain, listed here as a percentage, is the increase in coverage. Higher antenna gain improves the range of the signal for better communications. • **100%** - Sets the antenna gain at maximum output power. This has the highest level of power consumption. If you are using the NWD2105 on a notebook computer running on battery power, then using this power setting will drain the battery the fastest. • **75%** - Sets the antenna gain to medium-high output power. This is a decent comprimise between signal strength and power consumption. • **50%** - Sets the antenna gain to medium output power. The range is reduced but the power consumption is much less. • **25%** - Sets the antenna gain to low output power. This significantly reduces the transmission range but save considerable power. • **Lowest** - Sets the antenna gain to minimal output power. You are trading decent transmission range for significant power savings.
Bridge	Select the check box and an Ethernet adapter (network interface card (NIC)) on your computer from the drop-down list box. This allows you to connect your wireless network to the specified wired network. Note: This feature is not supported in Windows 2000.
Security type	Select a security type for your AP. Options are **DISABLE**, **WEP**, **WPA-PSK** and **WPA2-PSK**.
Save	Click to save the changes.
Cancel	Click to discard the changes.

5.4.1 Security Settings

When you configure the NWD2105 to act as an AP and wireless security is activated, the **Configuration** screen varies according to the encryption method used by your network.

5.4.1.1 Disable

This option indicates that no security services are enabled. Anyone within range of your AP can connect to it without having to enter a pre-shared key.

Note: When security settings are disabled in **AP Mode** and if you have a shared Internet connection via the **Bridge** feature (see page 80) or any shared folders on the computer that is hosting the AP, they will be available to anyone who is connected.

5.4.1.2 WEP Encryption

Configure WEP security with these options.

Figure 58 Security Setting: WEP

The following table describes the labels in this screen.

Table 23 Security Setting: WEP

LABEL	DESCRIPTION
Security type	Select **WEP** to enable this encryption type.
Authentication Type	Select an authentication method. Choices are **Open System** and **Shared Key**.
WEP	Select **64 Bits** or **128 Bits** for your WEP encryption type.
Transmit Key	Select a default WEP key to use for data encryption. Note: This feature is not available in Windows Vista.
Pass Phrase	If you select this transmit key option, enter a passphrase of up to 32 case-sensitive printable characters. As you enter the passphrase, the NWD2105 automatically generates four different transmit keys and displays the first in the key field below.

Table 23 Security Setting: WEP (continued)

LABEL	DESCRIPTION
Key 1-4	Select this option if you want to manually enter a transmit key. Enter the key in the field provided. If you select **64 Bits** in the **WEP** field. Enter either 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 11AA22BB33) for HEX key type. or Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for ASCII key type. If you select **128 Bits** in the **WEP** field, Enter either 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 00112233445566778899AABBCC) for HEX key type or Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for ASCII key type. Note: The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN. ASCII WEP keys are case sensitive.
Save	Click to save the changes.
Cancel	Click to discard the changes.

5.4.1.3 WPA-PSK/WPA2-PSK

Configure WPA-PSK and WPA2-PSK security with these options.

Figure 59 Security Setting: WPA-PSK/WPA2-PSK

The following table describes the labels in this screen.

Table 24 Security Setting: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Security Type	Select either **WPA-PSK** or **WPA2-PSK** to enable these encryption types.
Encryption Type	Select the encryption type (**TKIP** or **AES**) for data encryption.

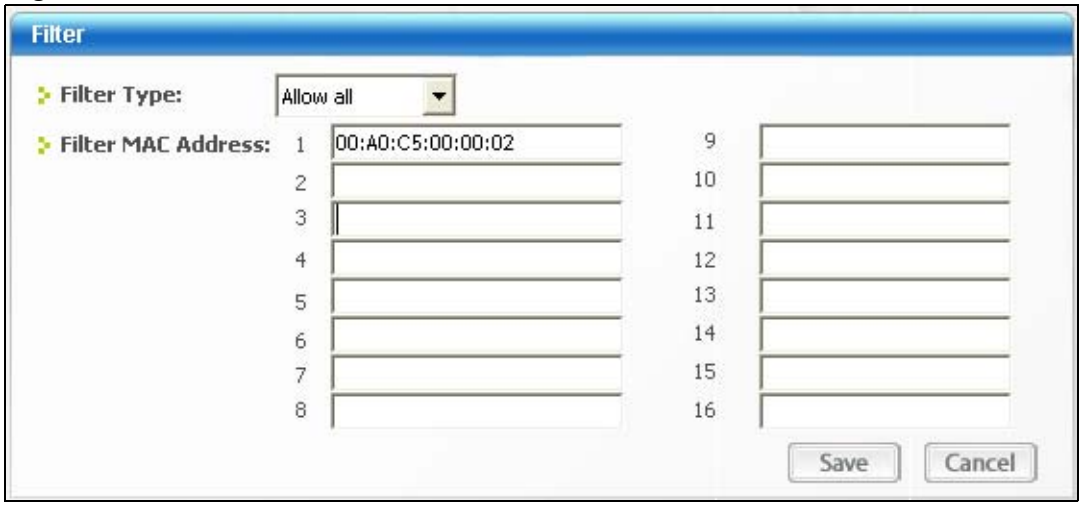
Table 24 Security Setting: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Pre-Shared Key	Type a pre-shared key (same as the AP or peer device) of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Save	Click to save the changes.
Cancel	Click to discard the changes.

5.5 The MAC Filter Screen

The **MAC Filter** screen allows you to configure the NWD2105 to give exclusive access to devices (**Allow all**) or exclude devices from connecting to the NWD2105 (**Reject all**). The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the device(s) to configure this screen.

Figure 60 The MAC Filter Screen



The following table describes the labels in this screen.

Table 25 MAC Filter

LABEL	DESCRIPTION
Filter Type	Define the filter action for the list of MAC addresses in the MAC address filter table. Select **Disable** to deactivate the MAC filter feature. Select **Reject all** to block access to the NWD2105, MAC addresses not listed will be allowed to access the NWD2105. Select **Allow all** to permit access to the NWD2105, MAC addresses not listed will be denied access to the NWD2105.
Filter MAC Address 1-16	Specify the MAC address(es) of the wireless station(s) that is allowed or denied association to the NWD2105. Enter six pairs of hexadecimal digits (separated by colons) in the range of “A-F”, “a-f” and “0-9” (for example, 00:A0:C5:00:00:02). If you enter an invalid MAC address, once you click **Save** to save the values, a warning screen will be displayed.
Save	Click to save the changes.
Cancel	Click to discard the changes.

6

Maintenance

6.1 Overview

This section describes how to uninstall or upgrade the ZyXEL utility.

6.1.1 What You Can Do in This Section

- Learn which version of the ZyXEL utility and device driver you're currently using. See Section 6.2 on page 86 for details.
- Remove the ZyXEL utility from your computer. See Section 6.3 on page 86 for details.
- Upgrade the ZyXEL utility. See Section 6.4 on page 87 for details.

6.1.2 What You Need to Know

The following term may help as you read through this section.

Device driver

A system file that lets other programs interact with a piece of hardware, or "device." You should never try to locate and install or uninstall device drivers yourself since they are modifications to an operating system at the core (or "kernel") level. Doing so could irreparably damage your installation.

6.1.3 Before You Begin

- Disconnect the NWD2105 if you are going to uninstall or upgrade the ZyXEL utility, save your work in any other open programs, and then close them.

6.2 The About Screen

The **About** screen displays driver and utility version numbers of the NWD2105. To display the screen as shown below, click the About ( ) button.

Figure 61 About

The following table describes the read-only fields in this screen.

Table 26 About

LABEL	DESCRIPTION
Driver Version	This field displays the version number of the NWD2105 driver.
Utility Version	This field displays the version number of the ZyXEL utility.

6.3 Uninstalling the ZyXEL Utility

Follow the steps below to remove (or uninstall) the ZyXEL utility from your computer.

Note: Before you uninstall the ZyXEL utility, take note of your current wireless configurations.

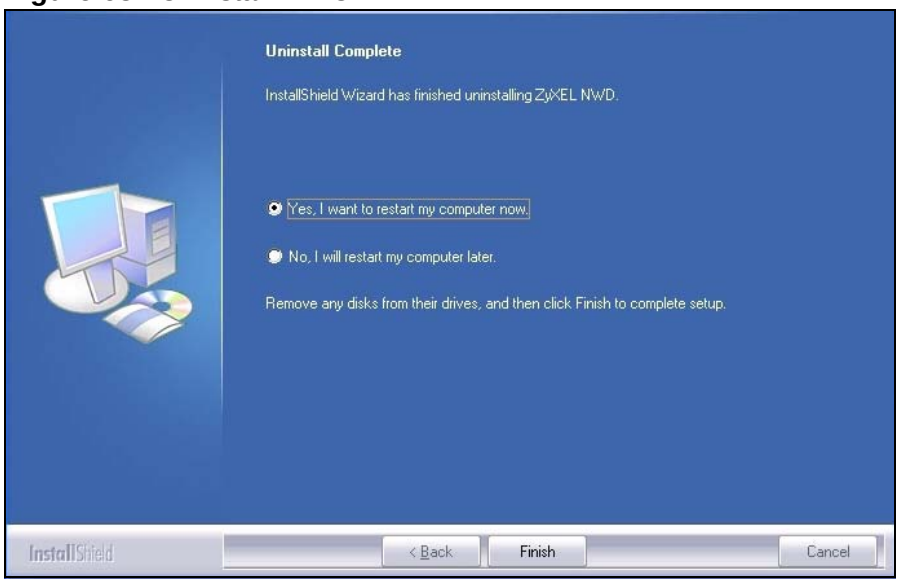
1 Click **Start** > **(All) Programs** > **Wireless N-lite USB Adapter Utility** > **Uninstall Wireless N-lite USB Adapter Utility**.

2 When prompted, click **OK** or **Yes** to remove the driver and the utility software.

Figure 62 Uninstall: Confirm

3 Click **Finish** to complete uninstalling the software and restart the computer when prompted.

Figure 63 Uninstall: Finish


Uninstall Complete
InstallShield Wizard has finished uninstalling ZyXEL NWD.
Yes, I want to restart my computer now.
No, I will restart my computer later.
Remove any disks from their drives, and then click Finish to complete setup.
InstallShield
< Back
Finish
Cancel

6.4 Upgrading the ZyXEL Utility

Note: Before you uninstall the ZyXEL utility, take note of your current wireless configurations.

To perform the upgrade, follow the steps below.

1 Download the latest version of the utility from the ZyXEL web site and save the file on your computer.

2 Follow the steps in Section 6.3 on page 86 to remove the current ZyXEL utility from your computer.

3 Restart your computer when prompted.

4 Disconnect the NWD2105 from your computer.

5 Double-click on the setup program for the new utility to start the ZyXEL utility installation.

6 Insert the NWD2105 and check the version numbers in the **About** screen to make sure the new utility is installed properly.

PART II
Troubleshooting and Specifications

Troubleshooting (91)

Product Specifications (95)

7

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- Accessing the ZyXEL Utility
- Link Quality
- Problems Communicating with Other Computers

7.1 Power, Hardware Connections, and LEDs

The NWD2105 does not turn on. None of the LEDs turn on.

1. Make sure the NWD2105 is correctly installed (refer to your Quick Start Guide).
2. Restart the computer to which the NWD2105 is attached.
3. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.2 on page 18.
2. Check the hardware connection. See the Quick Start Guide and Section 1.2 on page 18.
3. Restart the computer to which the NWD2105 is attached.
4. If the problem continues, contact the vendor.

7.2 Accessing the ZyXEL Utility

I cannot access the ZyXEL Utility

1. Make sure the NWD2105 is properly inserted and the LEDs are on. Refer to the Quick Start Guide for information on how to properly connect the NWD2105.
2. Use the **Device Manager** to check for possible hardware conflicts. Click **Start** > **Settings** > **Control Panel** > **System** > **Hardware** > **Device Manager**. Verify the status of the NWD2105 under **Network Adapter** (steps may vary depending on the version of Windows).
3. Install the NWD2105 on another computer.
4. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

7.3 Link Quality

The link quality and/or signal strength is poor.

1. Scan for and connect to another AP with a better link quality using the **Site Survey** screen.
2. Move your computer closer to the AP or the peer computer(s) within the transmission range.
3. There may be too much radio interference (for example from a microwave oven, or another AP using the same channel) around your wireless network. Lower the output power of each AP.
4. Make sure there are not too many wireless stations connected to a wireless network.

7.4 Problems Communicating with Other Computers

The computer with the NWD2105 installed cannot communicate with the other computer(s).

In Infrastructure Mode

- Make sure that the AP and the associated computers are turned on and working properly.
- Make sure the NWD2105 computer and the associated AP use the same SSID.
- Change the AP and the associated wireless clients to use another radio channel if interference is high.
- Make sure that the computer and the AP share the same security option and key. Verify the settings in the **Profile Security Setting** screen.
- If you are using WPA(2) or WPA(2)-PSK security, try changing your encryption type from TKIP to AES or vice versa.

In Ad-Hoc Mode

- Verify that the peer computer(s) is turned on.
- Make sure the NWD2105 computer and the peer computer(s) are using the same SSID and channel.
- Make sure that the computer and the peer computer(s) share the same security settings.
- Change the wireless clients to use another radio channel if interference is high.

8

Product Specifications

Table 27 Product Specifications

PHYSICAL AND ENVIRONMENTAL	
Product Name	NWD2105 Wireless N-lite USB Adapter
Interface	USB 2.0
Standards	IEEE 802.11b IEEE 802.11g IEEE 802.11n
Operating Frequency	2.4GHZ
Antenna Type	Chip
Operating Temperature	0 - 50 degrees Celsius
Storage Temperature	-30 - 70 degrees Celsius
Operating Humidity	20 - 90% (non-condensing)
Storage Humidity	10 - 90% (non-condensing)
Voltage	5V
Power Saving Mode	Yes
Current Consumption	Transmit: <300 mA Receive: <160 mA
Device Weight	3 g
Device Dimensions	18 mm (L) x 6 mm (W) x 36 mm (H)
RADIO SPECIFICATIONS	

Table 27 Product Specifications (continued)

Transmit Power (+/- 1.5 dB)	802.11b: 1/2/5.5/11M: 18.5 dBm 802.11g: 54/48M: 15dBm 24/36M: 15dBm 12/18M: 16dBm 6/9M: 16.5 dBm 802.11n: @ HT20 MCS0~MCS07: 15.5 dBm @ HT40 MCS0~MCS07: 15.5 dBm
Receiver Sensitivity	802.11b: 11Mbps at -82dBm 802.11g: 54Mbps at -68dBm 802.11n: HT20 at -64dBm HT40 at -62dBm
WIRELESS STANDARDS	
IEEE 802.11b	Dynamically shifts between 11, 5.5, 2, and 1 Mbps network speed.
Operation Frequency	2.412GHz~2.472GHz
Operation Channels	N. America &Taiwan 2.412GHz~ 2.462GHz 1-11 Euro ETSI 2.412GHz~ 2.472GHz 1-13
IEEE 802.11g	Dynamically shifts between 54, 48, 36, 24, 18, 12, 9 and 6 Mbps network speed.
Operation Frequency	2.412GHz~2.472GHz
Operation Channels	N. America &Taiwan 2.412GHz~ 2.462GHz 1-11 Euro ETSI 2.412GHz~ 2.472GHz 1-13
IEEE 802.11n	
Downstream data rate	150 Mbps
Upstream data rate	150 Mbps
Operation Frequency	2.412GHz~ 2.472GHz 1-13

Table 27 Product Specifications (continued)

Operation Channels	N. America & Taiwan HT20 2.412GHz~ 2.462GHz 1-11 N. America & Taiwan HT40 2.422GHz~ 2.452GHz 3-9 Euro ETSI HT20 2.412GHz~ 2.472GHz 1-13 Euro ETSI HT40 2.422GHz~ 2.462GHz 3-11
Networking Mode	Infrastructure, Ad-Hoc, SoftAP Support
Approvals	Safety European Union: EN60950-1 (CE-LVD) EMI United States: FCC Part 15B Class B Canada: ICES-003 European Union: CE EN 55022 Class B Australia: C-Tick EMS European Union: CE EN55024 RF United States: FCC Part 15C Canada: RSS-210 European Union: CE EN 300 328 Taiwan: NCC LP0002 Wi-Fi Certification 11 b/g/n WPA/WPA2/WPS Microsoft Certification WHQL: Windows 7 (32- and 64-bit), Windows Vista (32- and 64-bit), Windows XP (32- and 64-bit), Windows 2000
SOFTWARE SPECIFICATIONS	
Device Drivers	Windows 7 (32- and 64-bit) Windows Vista (32- and 64-bit) Windows XP (32- and 64-bit) Windows 2000 Mac OS X (10.3/10.4/10.5)
WIRELESS FEATURES	
Wireless Security	WEP 64bit, 128bit, WPA, WPA-PSK, WPA2, WPA2-PSK 802.1x (EAP-TLS, EAP-TTLS, EAP-PEAP), WPS. Note: EAP-TTLS is not supported in Windows Vista

Table 27 Product Specifications (continued)

Wireless QoS	Wi-Fi Multi Media (WMM)
Wi-Fi Protected Setup (WPS)	Push button configuration Use device's PIN Use AP or Router's PIN
Other	WMM power-saving support Compatible with Windows Zero Configuration

PART III Appendices and Index

Note: The appendices provide general information. Some details may not apply to your NWD2105.

Setting Up Your Computer's IP Address (101)

Wireless LANs (131)

Windows Wireless Management (147)

Wireless for Windows 7 (173)

Legal Information (179)

Index (185)

A

Setting Up Your Computer's IP Address

Note: Your specific NWD2105 may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

In this appendix, you can set up an IP address for:

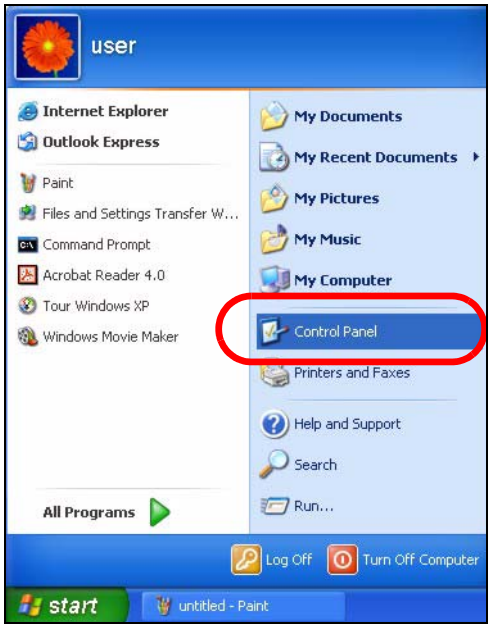
- Windows XP/NT/2000 on page 101
- Windows Vista on page 105
- Windows 7 on page 109
- Mac OS X: 10.3 and 10.4 on page 113
- Mac OS X: 10.5 and 10.6 on page 117
- Linux: Ubuntu 8 (GNOME) on page 120
- Linux: openSUSE 10.3 (KDE) on page 125

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

1 Click **Start** > **Control Panel**.

Figure 64 Windows XP: Start Menu

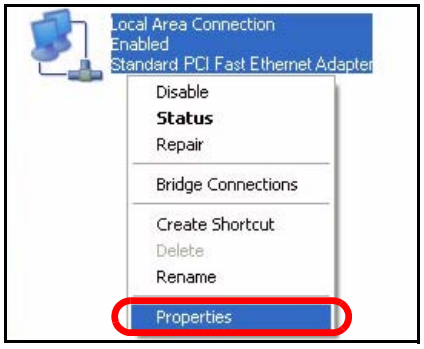


2 In the **Control Panel**, click the **Network Connections** icon.

Figure 65 Windows XP: Control Panel

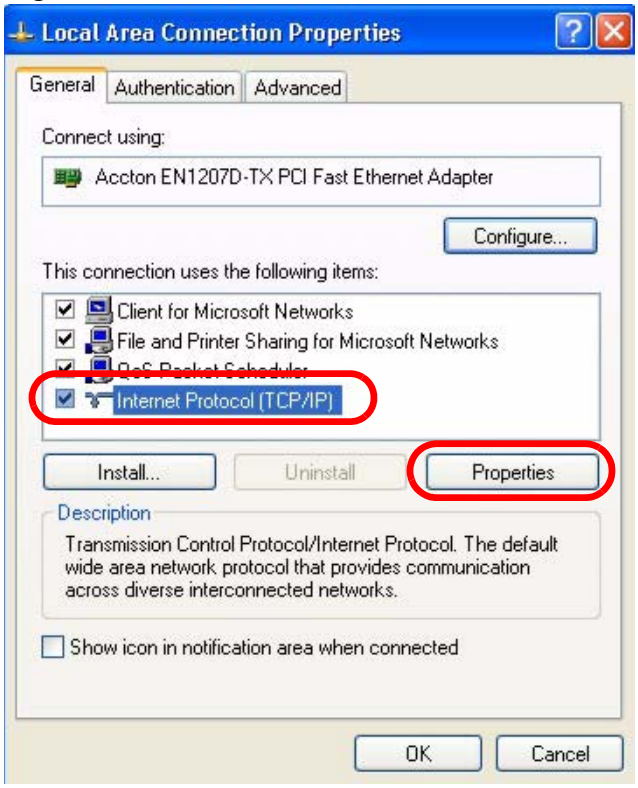
3 Right-click **Local Area Connection** and then select **Properties**.

Figure 66 Windows XP: Control Panel > Network Connections > Properties



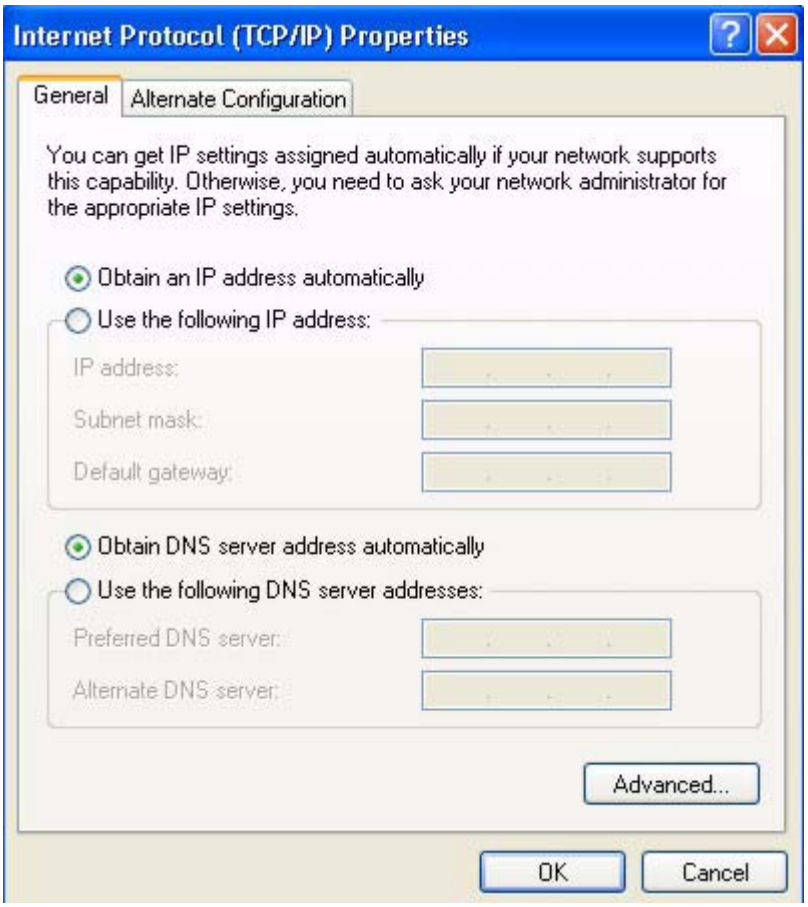
4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 67 Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens.

Figure 68 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

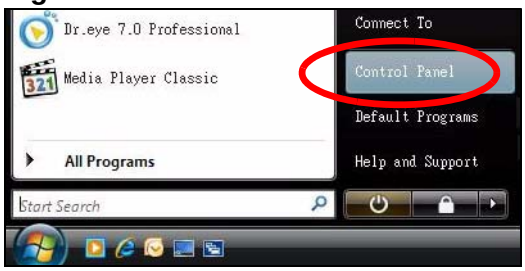
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

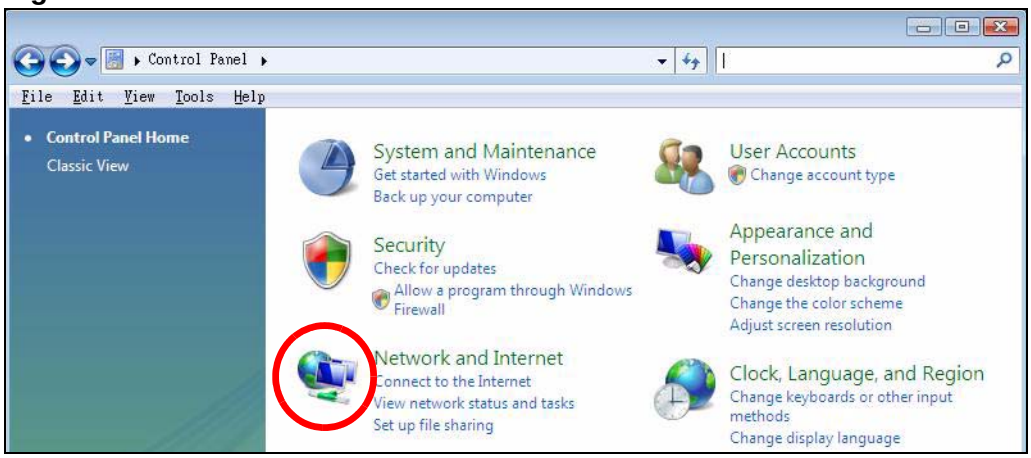
1 Click **Start** > **Control Panel**.

Figure 69 Windows Vista: Start Menu



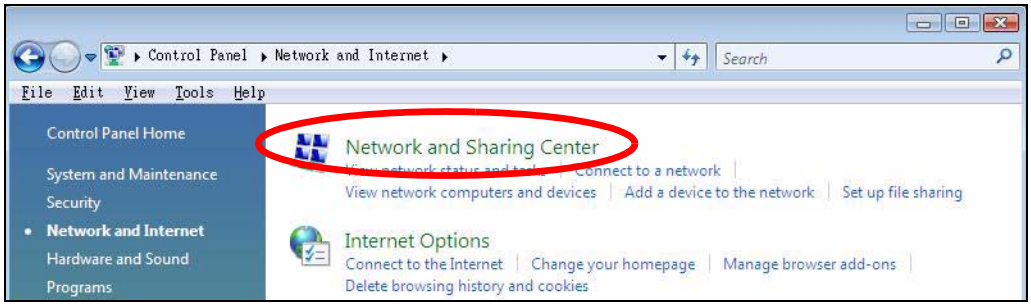
2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 70 Windows Vista: Control Panel



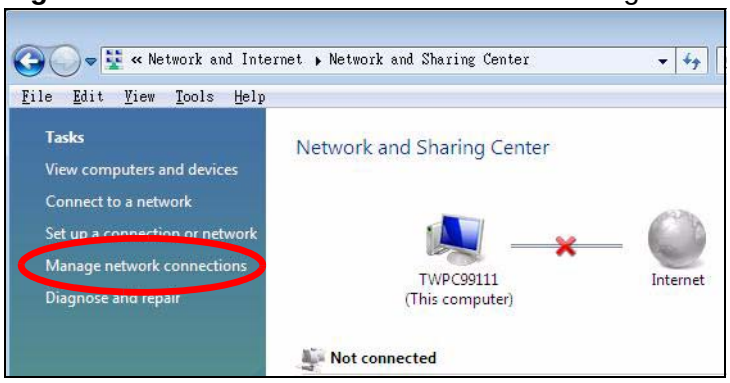
3 Click the **Network and Sharing Center** icon.

Figure 71 Windows Vista: Network And Internet



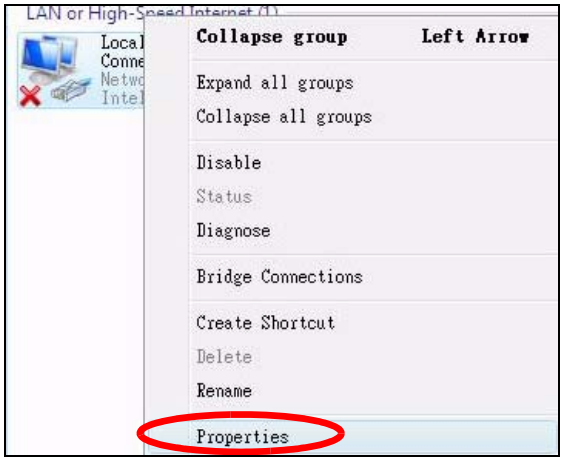
4 Click **Manage network connections**.

Figure 72 Windows Vista: Network and Sharing Center



5 Right-click **Local Area Connection** and then select **Properties**.

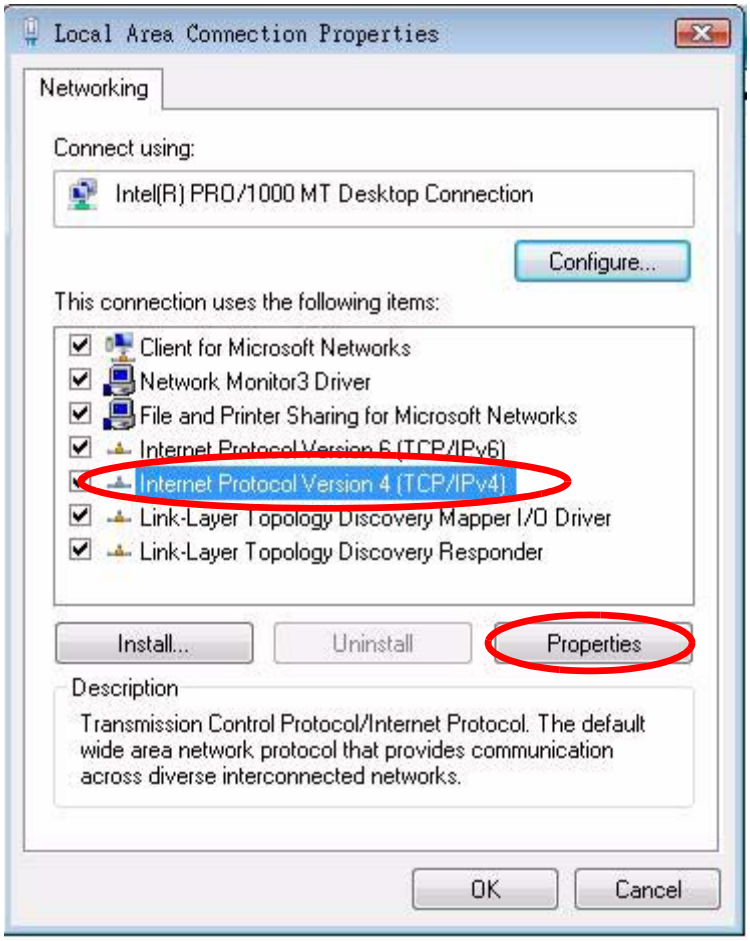
Figure 73 Windows Vista: Network and Sharing Center



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

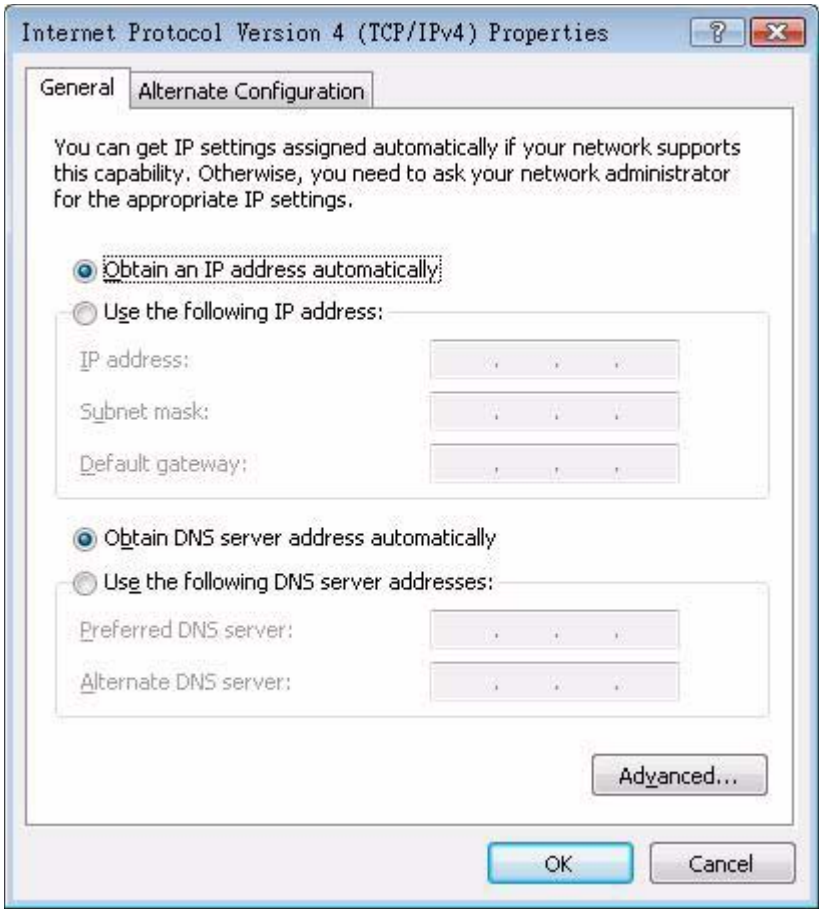
6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 74 Windows Vista: Local Area Connection Properties



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 75 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

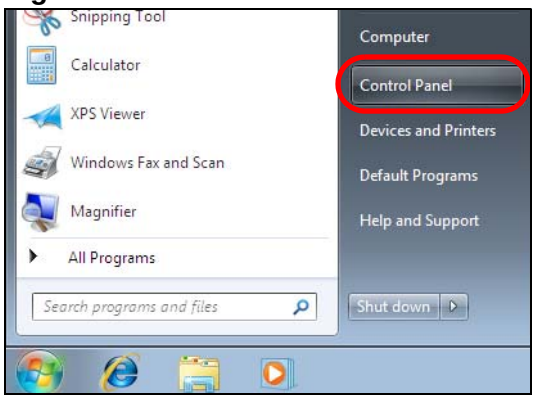
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows 7

This section shows screens from Windows 7 Enterprise.

1 Click **Start** > **Control Panel**.

Figure 76 Windows 7: Start Menu

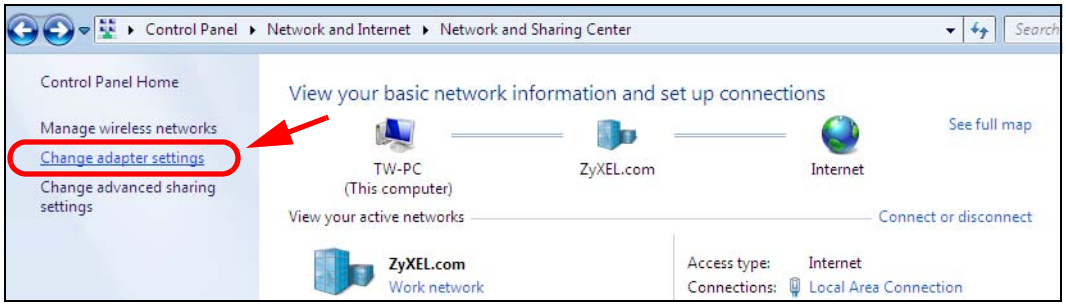


2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

Figure 77 Windows 7: Control Panel

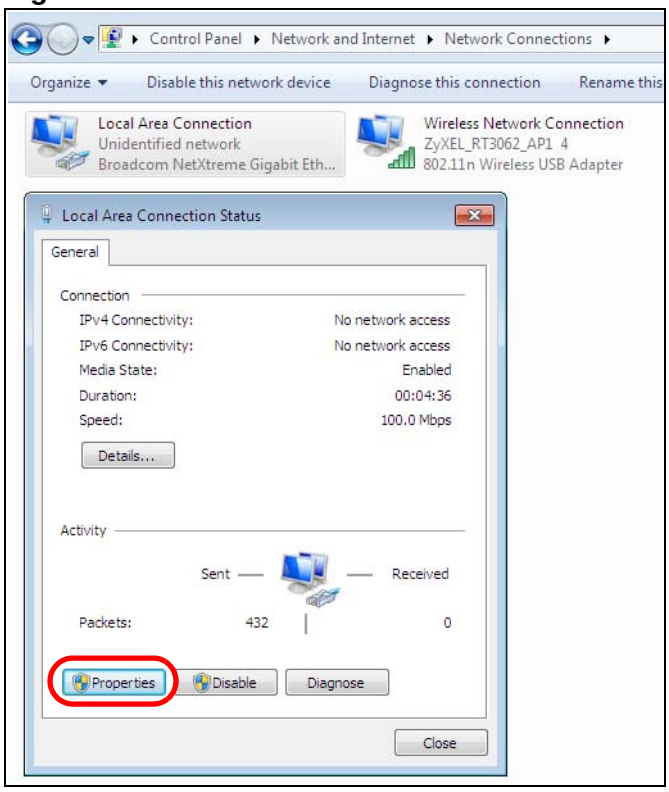
3 Click **Change adapter settings**.

Figure 78 Windows 7: Network And Sharing Center



4 Double click **Local Area Connection** and then select **Properties**.

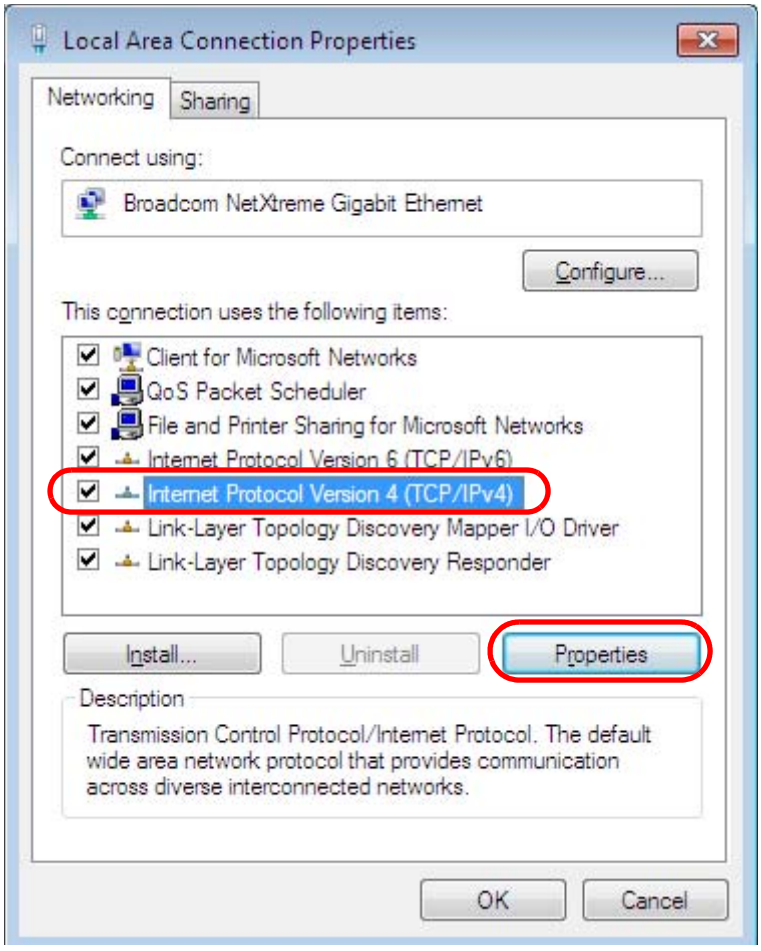
Figure 79 Windows 7: Local Area Connection Status



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

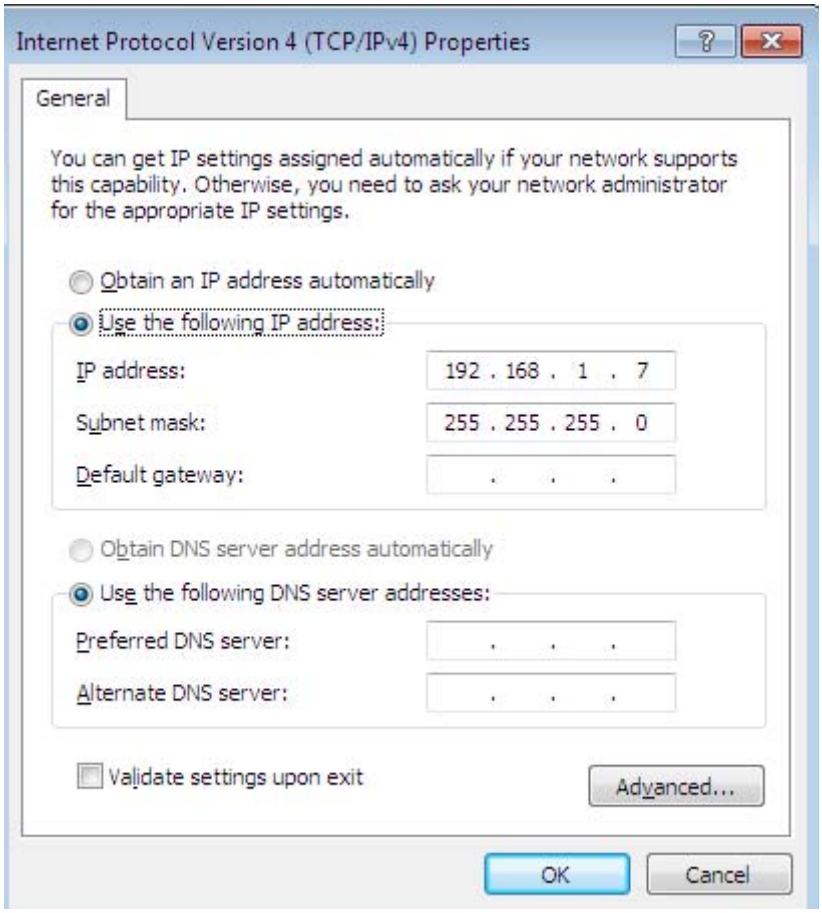
5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 80 Windows 7: Local Area Connection Properties



6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 81 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 7
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

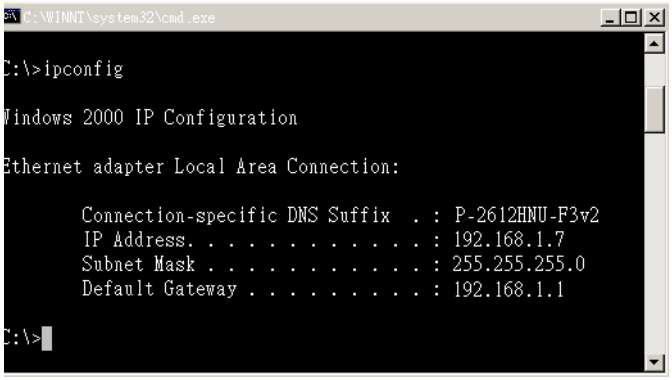
Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

3 The IP settings are displayed as follows.

Figure 82 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties

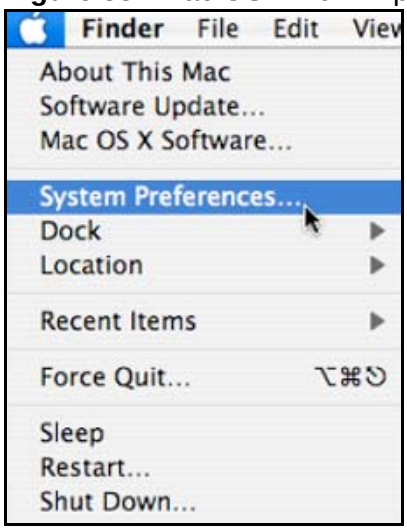

C:\WINNT\system32\cmd.exe
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : P-2612HNU-F3v2
IP Address. . . . . : 192.168.1.7
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\>

Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

Figure 83 Mac OS X 10.4: Apple Menu

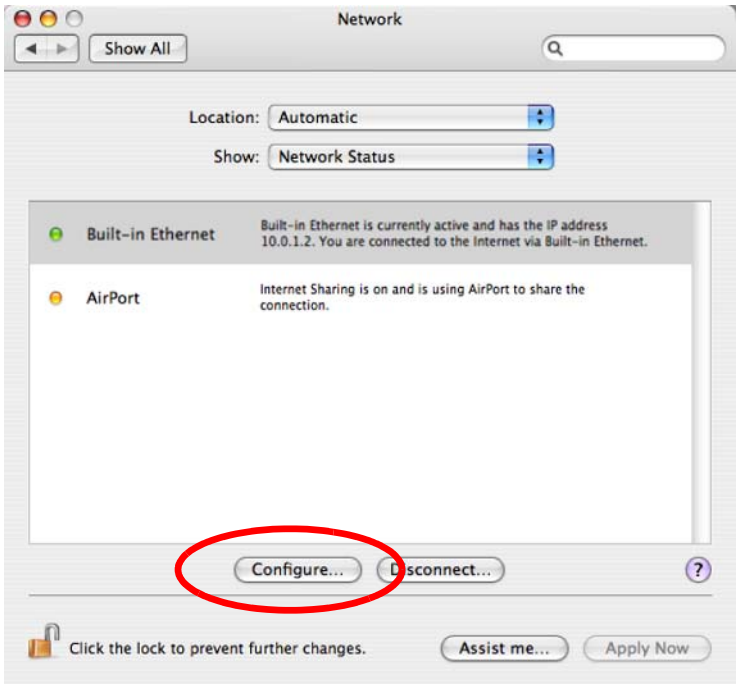


2 In the **System Preferences** window, click the **Network** icon.

Figure 84 Mac OS X 10.4: System Preferences

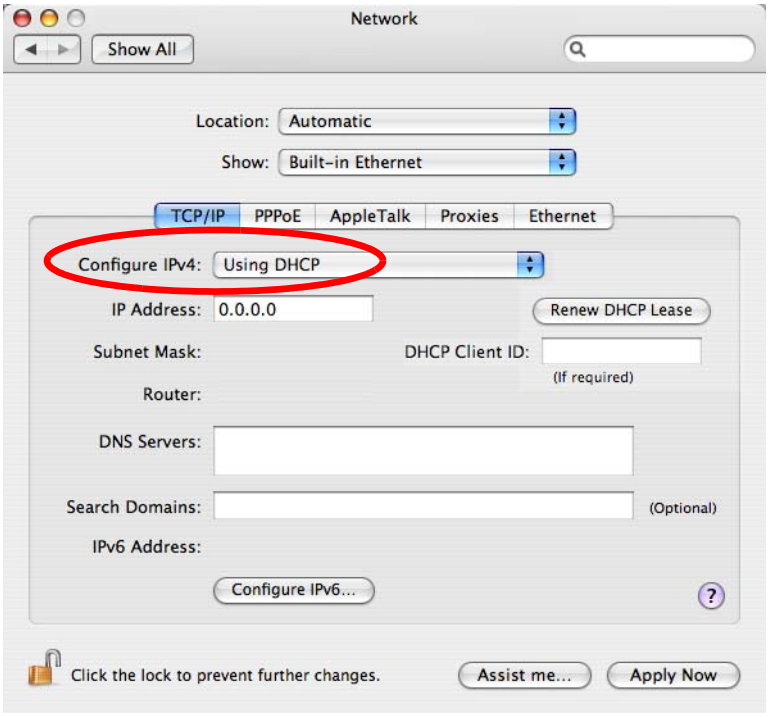
3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

Figure 85 Mac OS X 10.4: Network Preferences


Network
Show All
Location: Automatic
Show: Network Status
Built-in Ethernet
Built-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the Internet via Built-in Ethernet.
AirPort
Internet Sharing is on and is using AirPort to share the connection.
Configure...
Disconnect...
Click the lock to prevent further changes.
Assist me...
Apply Now

4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

Figure 86 Mac OS X 10.4: Network Preferences > TCP/IP Tab.

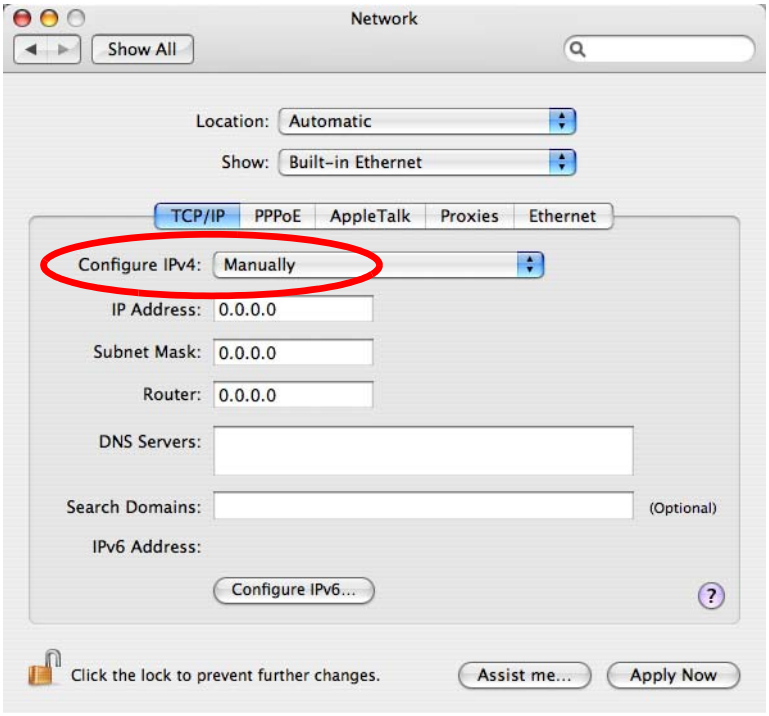


5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.

- In the **Router** field, type the IP address of your device.

Figure 87 Mac OS X 10.4: Network Preferences > Ethernet

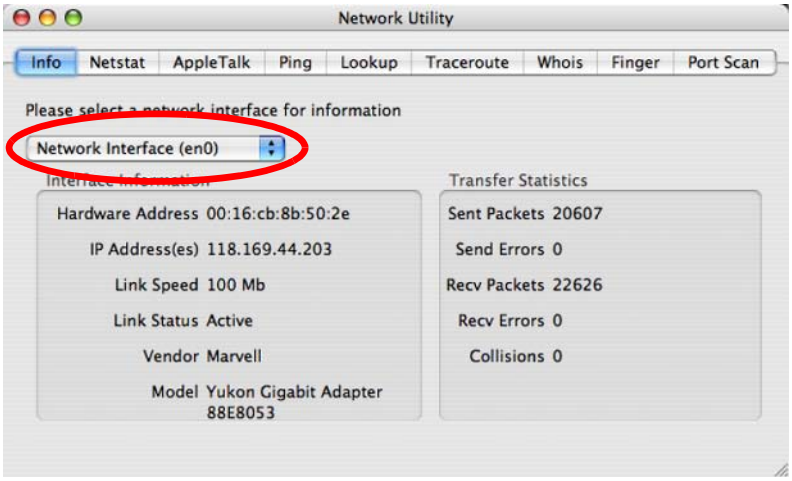


6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 88 Mac OS X 10.4: Network Utility

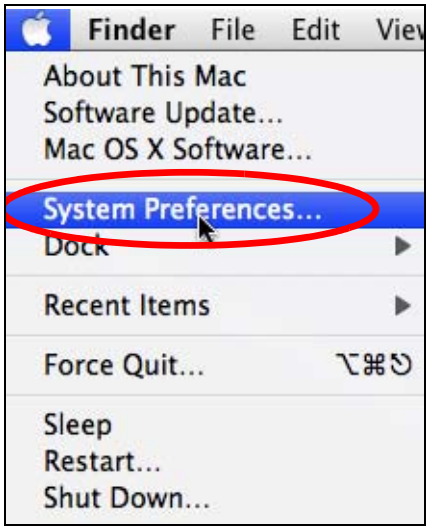


Mac OS X: 10.5 and 10.6

The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

1 Click **Apple** > **System Preferences**.

Figure 89 Mac OS X 10.5: Apple Menu

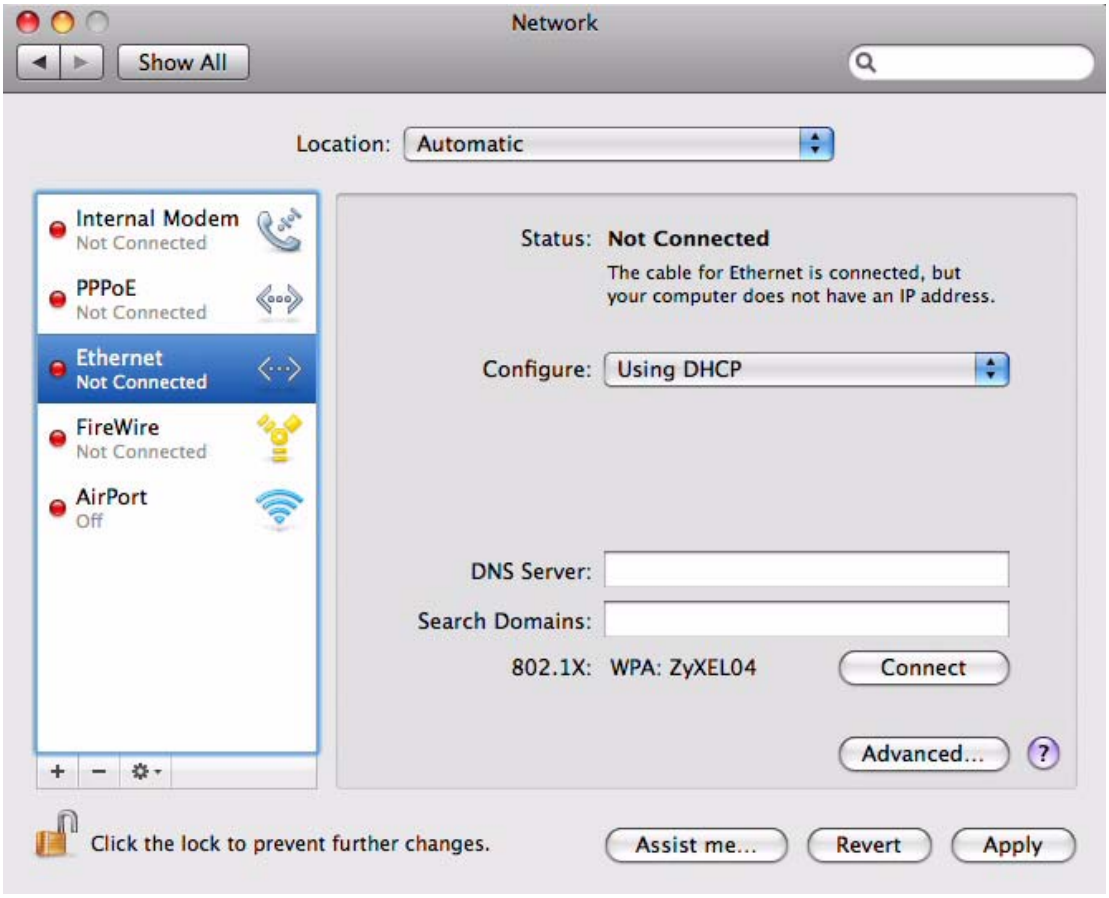


2 In **System Preferences**, click the **Network** icon.

Figure 90 Mac OS X 10.5: Systems Preferences

3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

Figure 91 Mac OS X 10.5: Network Preferences > Ethernet



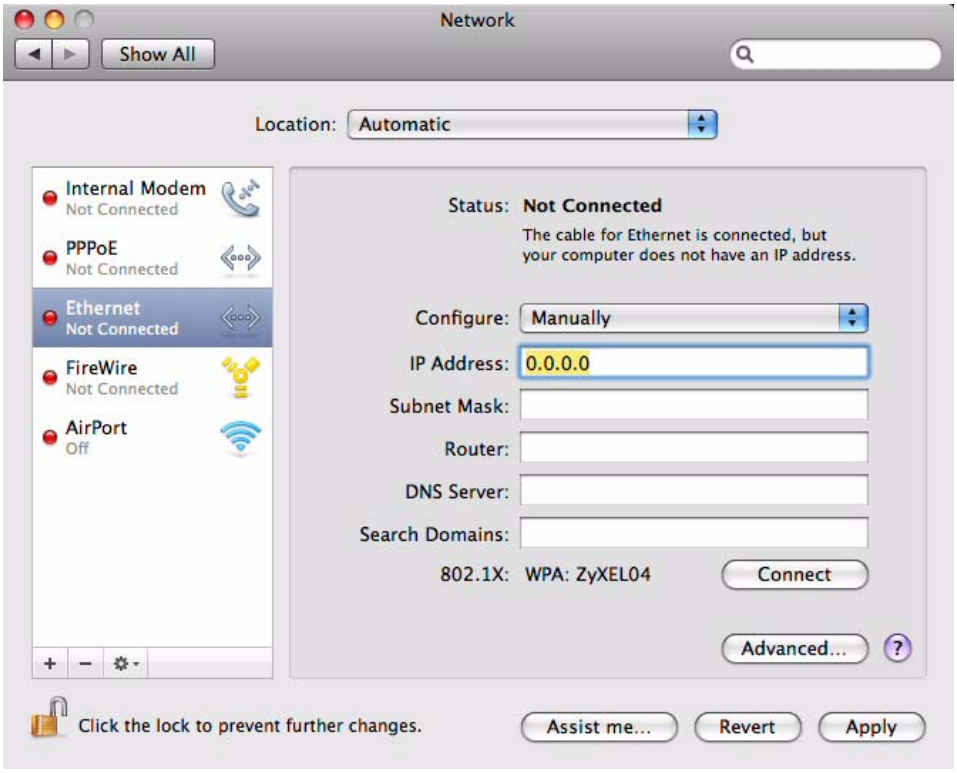
4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.

- In the **Router** field, enter the IP address of your NWD2105.

Figure 92 Mac OS X 10.5: Network Preferences > Ethernet

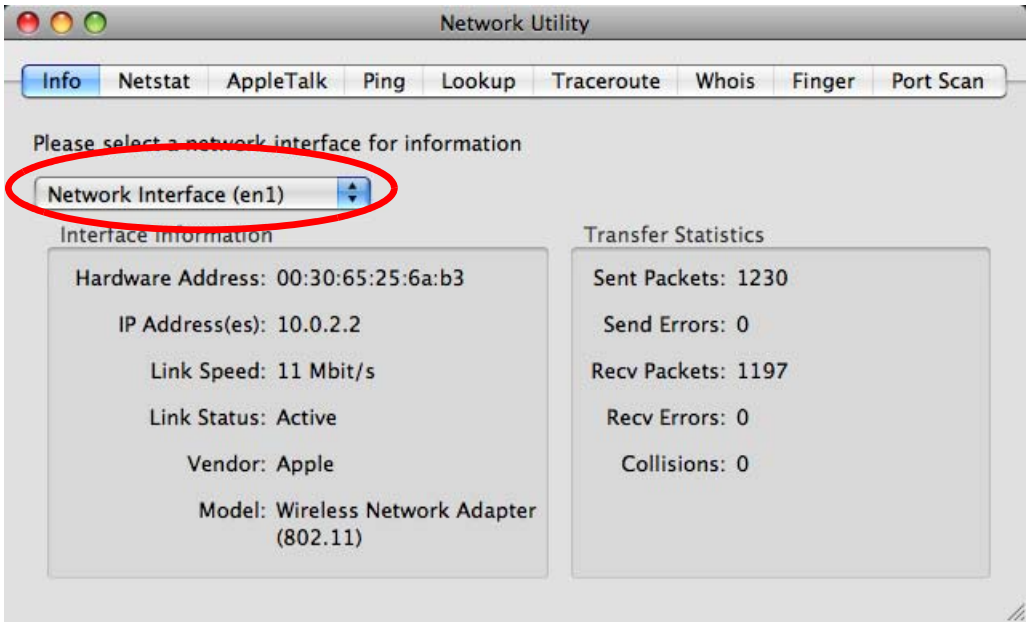


6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 93 Mac OS X 10.5: Network Utility



Linux: Ubuntu 8 (GNOME)

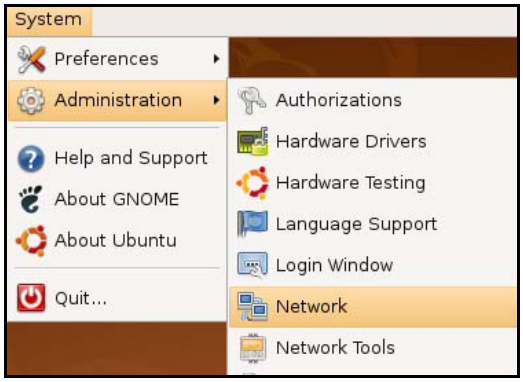
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

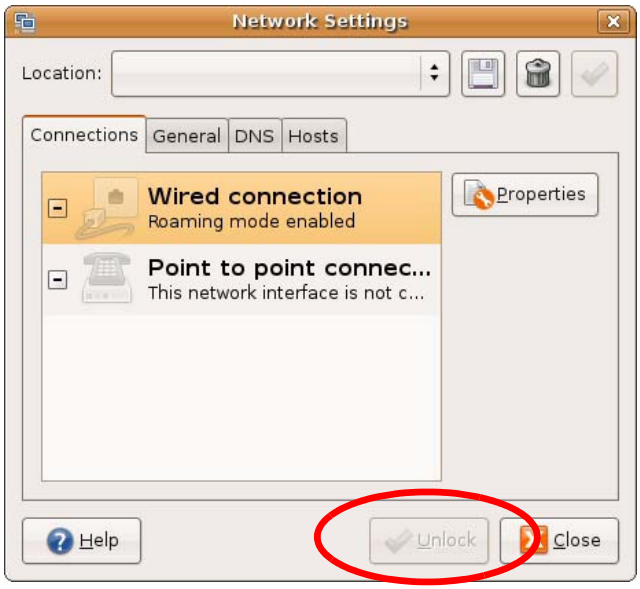
1 Click **System > Administration > Network**.

Figure 94 Ubuntu 8: System > Administration Menu



2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 95 Ubuntu 8: Network Settings > Connections



3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Figure 96 Ubuntu 8: Administrator Account Authentication

Authenticate
System policy prevents modifying the configuration
An application is attempting to perform an action that requires privileges. Authentication as one of the users below is required to perform this action.
C.J.,,,, (chris)
Password for chris:
Details
Cancel
Authenticate

4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 97 Ubuntu 8: Network Settings > Connections

5 The **Properties** dialog box opens.

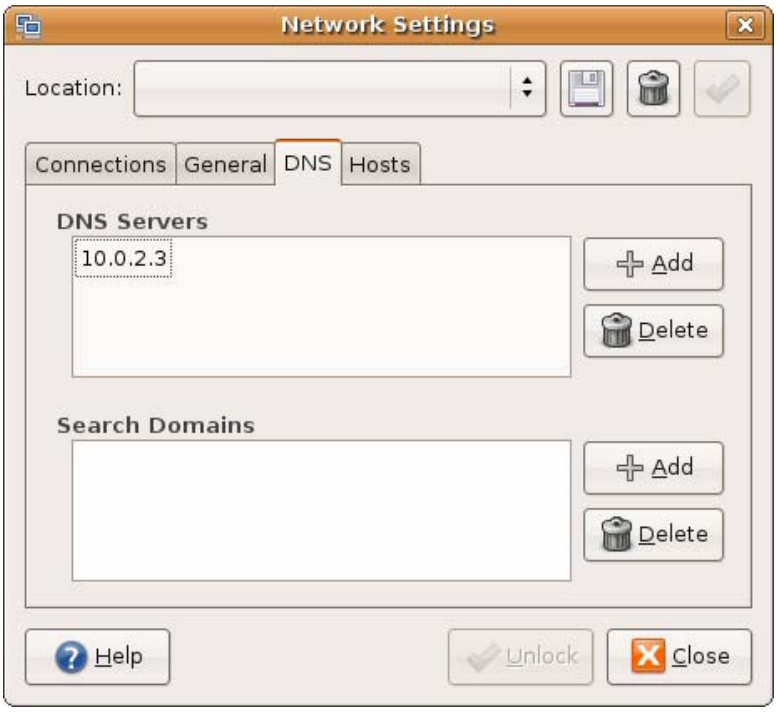
Figure 98 Ubuntu 8: Network Settings > Properties

- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

Figure 99 Ubuntu 8: Network Settings > DNS



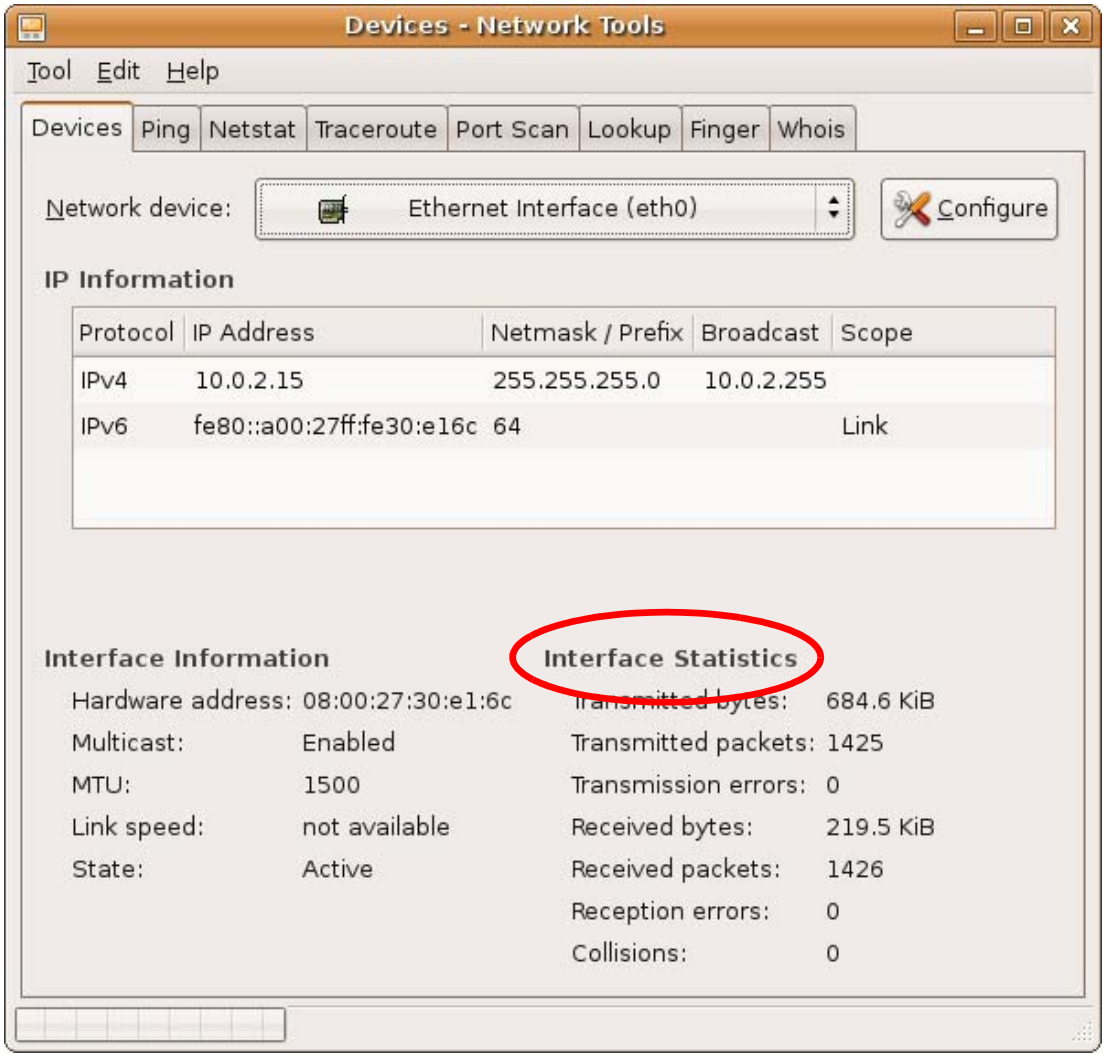
8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices**

tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 100 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

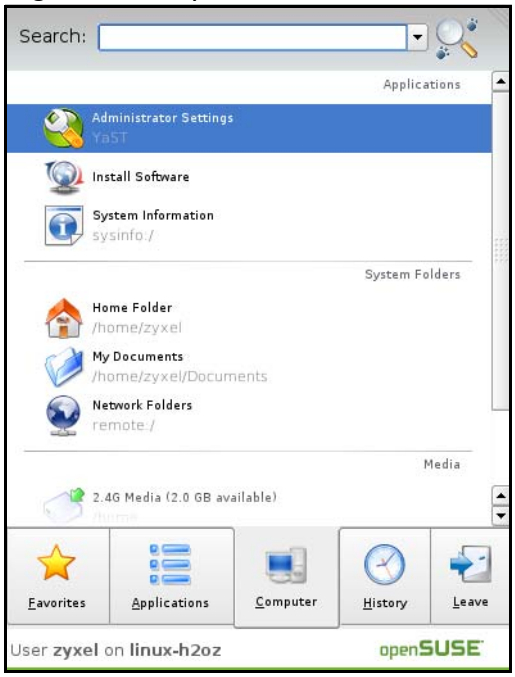
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

1 Click **K Menu > Computer > Administrator Settings (YaST)**.

Figure 101 openSUSE 10.3: K Menu > Computer Menu

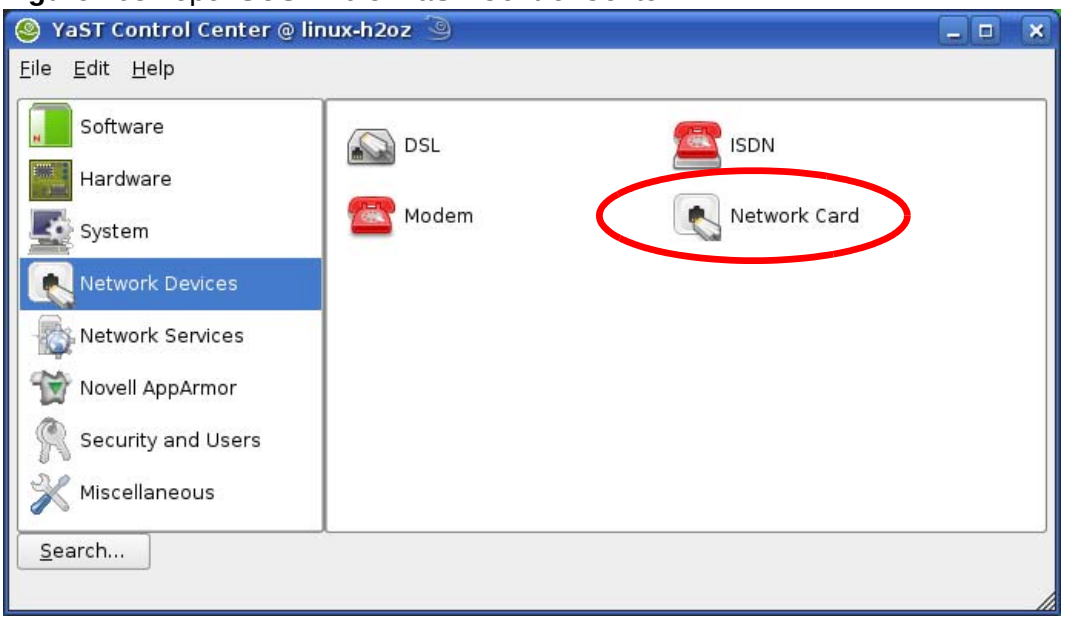


2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 102 openSUSE 10.3: K Menu > Computer Menu

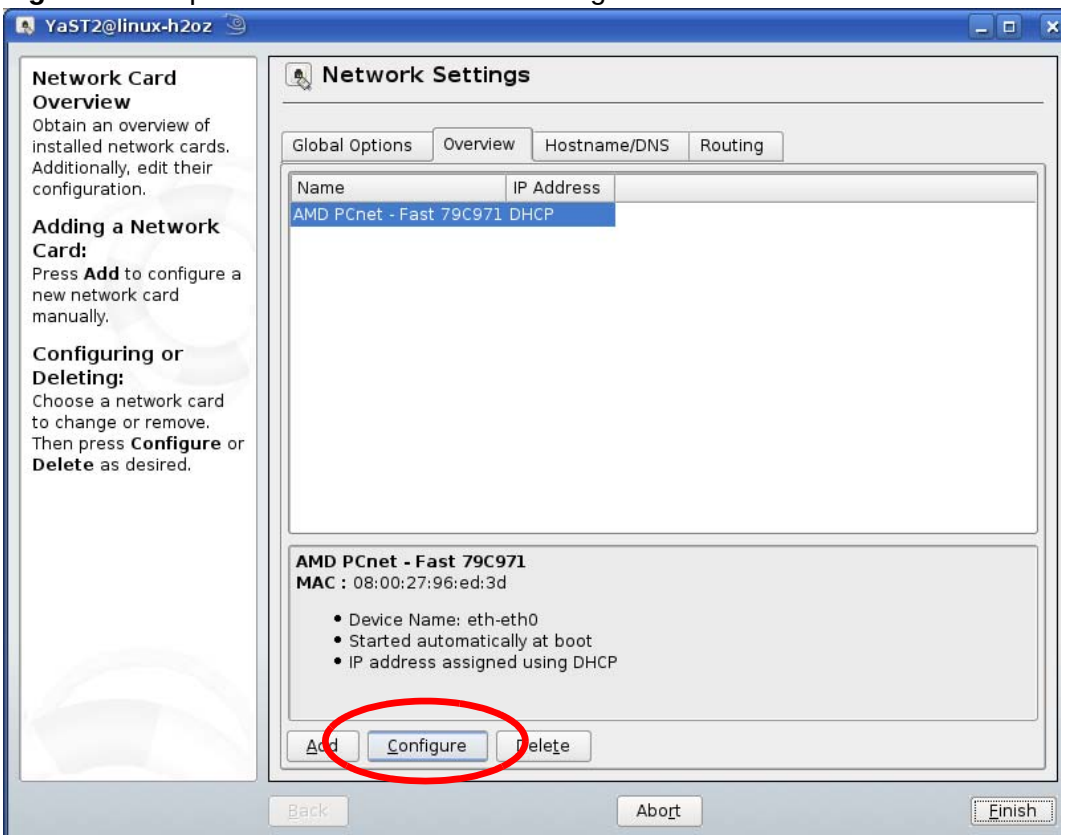
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 103 openSUSE 10.3: YaST Control Center



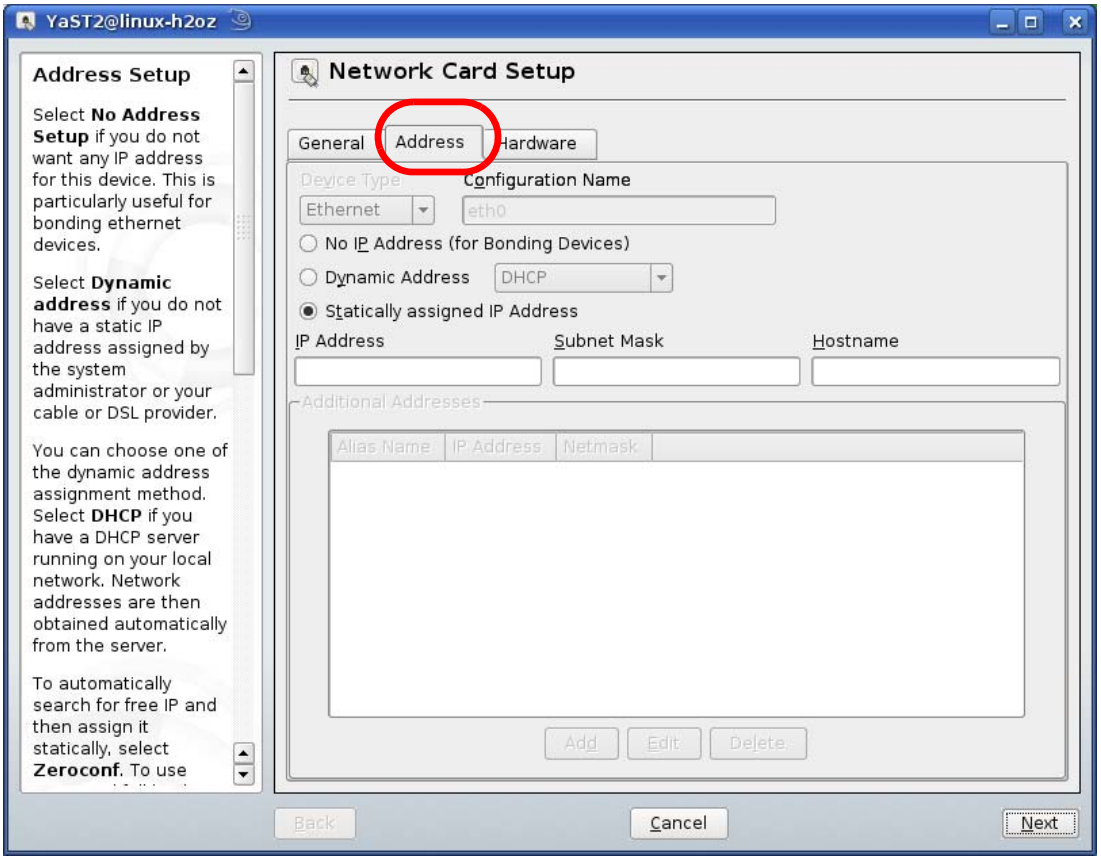
4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

Figure 104 openSUSE 10.3: Network Settings



5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 105 openSUSE 10.3: Network Card Setup


YaST2@linux-h2oz
Address Setup
Select No Address Setup if you do not want any IP address for this device. This is particularly useful for bonding ethernet devices.
Select Dynamic address if you do not have a static IP address assigned by the system administrator or your cable or DSL provider.
You can choose one of the dynamic address assignment method. Select DHCP if you have a DHCP server running on your local network. Network addresses are then obtained automatically from the server.
To automatically search for free IP and then assign it statically, select Zeroconf. To use
Network Card Setup
General
Address
Hardware
Device Type
Configuration Name
Ethernet
eth0
No IP Address (for Bonding Devices)
Dynamic Address
DHCP
Statically assigned IP Address
IP Address
Subnet Mask
Hostname
Additional Addresses
Alias Name
IP Address
Netmask
Add
Edit
Delete
Back
Cancel
Next

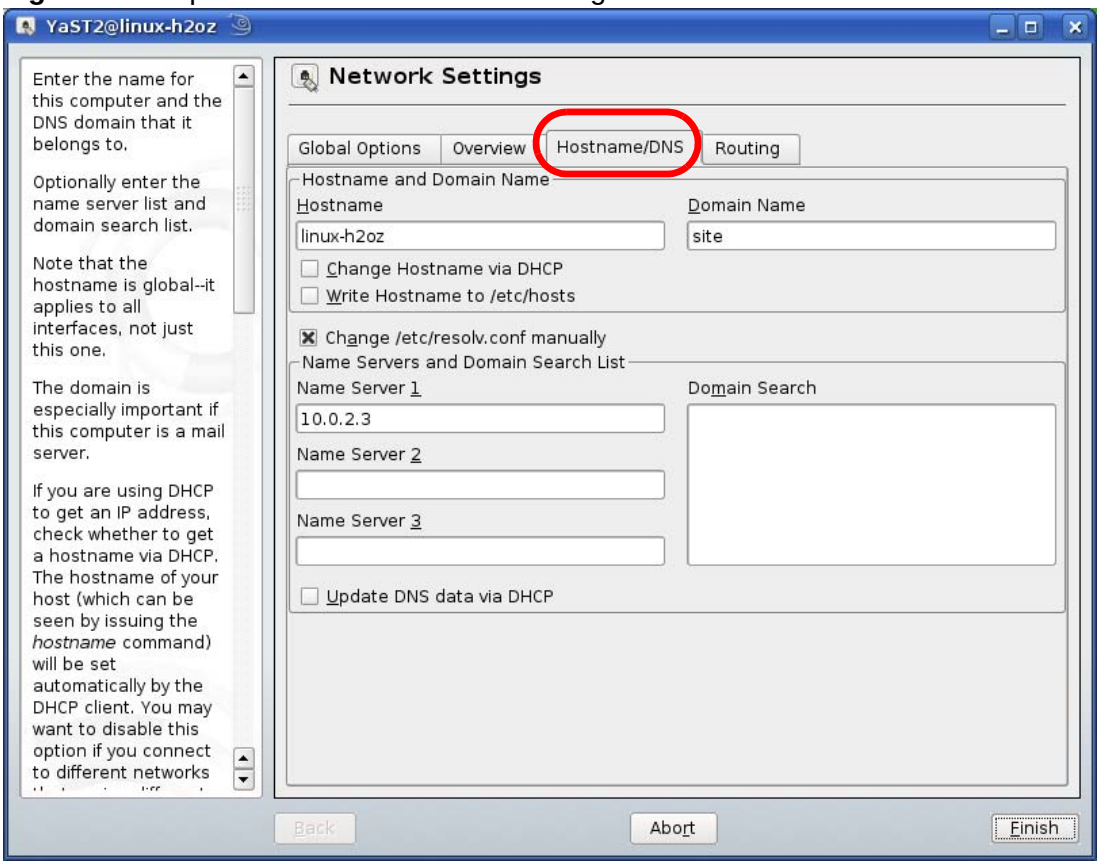
6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

Figure 106 openSUSE 10.3: Network Settings


YaST2@linux-h2oz
Enter the name for this computer and the DNS domain that it belongs to.
Optionally enter the name server list and domain search list.
Note that the hostname is global--it applies to all interfaces, not just this one.
The domain is especially important if this computer is a mail server.
If you are using DHCP to get an IP address, check whether to get a hostname via DHCP. The hostname of your host (which can be seen by issuing the hostname command) will be set automatically by the DHCP client. You may want to disable this option if you connect to different networks
Network Settings
Global Options
Overview
Hostname/DNS
Routing
Hostname and Domain Name
Hostname
linux-h2oz
Domain Name
site
Change Hostname via DHCP
Write Hostname to /etc/hosts
Change /etc/resolv.conf manually
Name Servers and Domain Search List
Name Server 1
10.0.2.3
Domain Search
Name Server 2
Name Server 3
Update DNS data via DHCP
Back
Abort
Finish

9 Click **Finish** to save your settings and close the window.

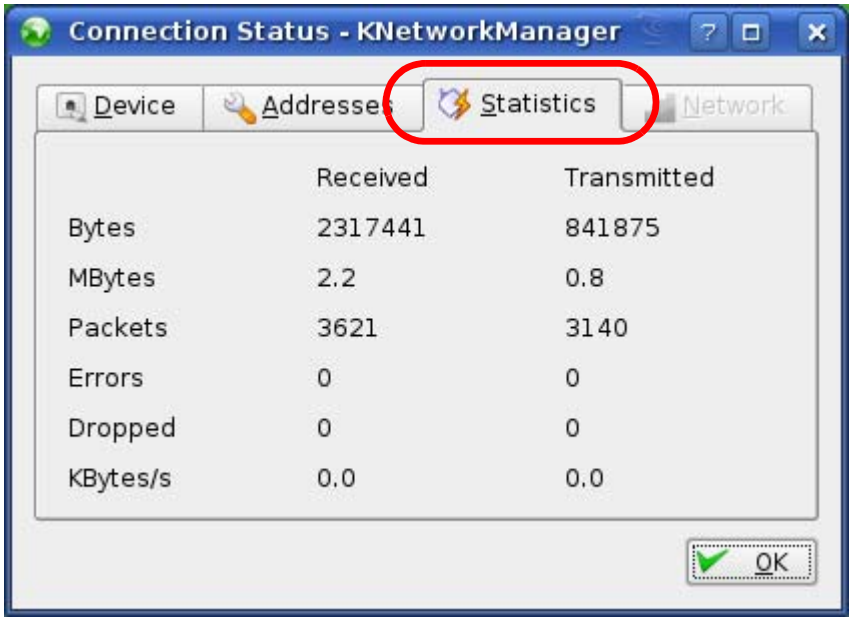
Verifying Settings

Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 107 openSUSE 10.3: KNetwork Manager

When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 108 openSUSE: Connection Status - KNetwork Manager



B

Wireless LANs

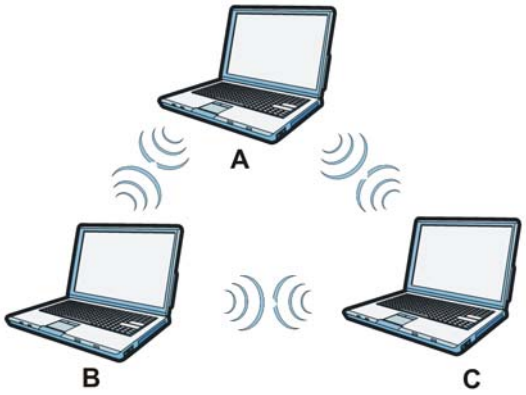
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 109 Peer-to-Peer Communication in an Ad-hoc Network



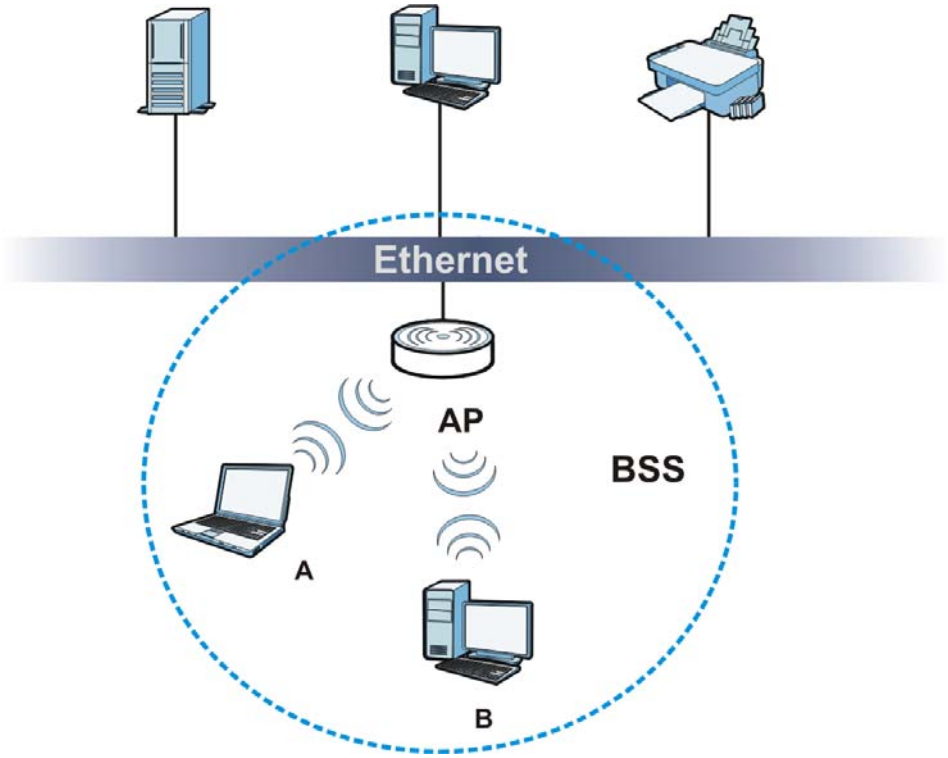
BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate

with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 110 Basic Service Set



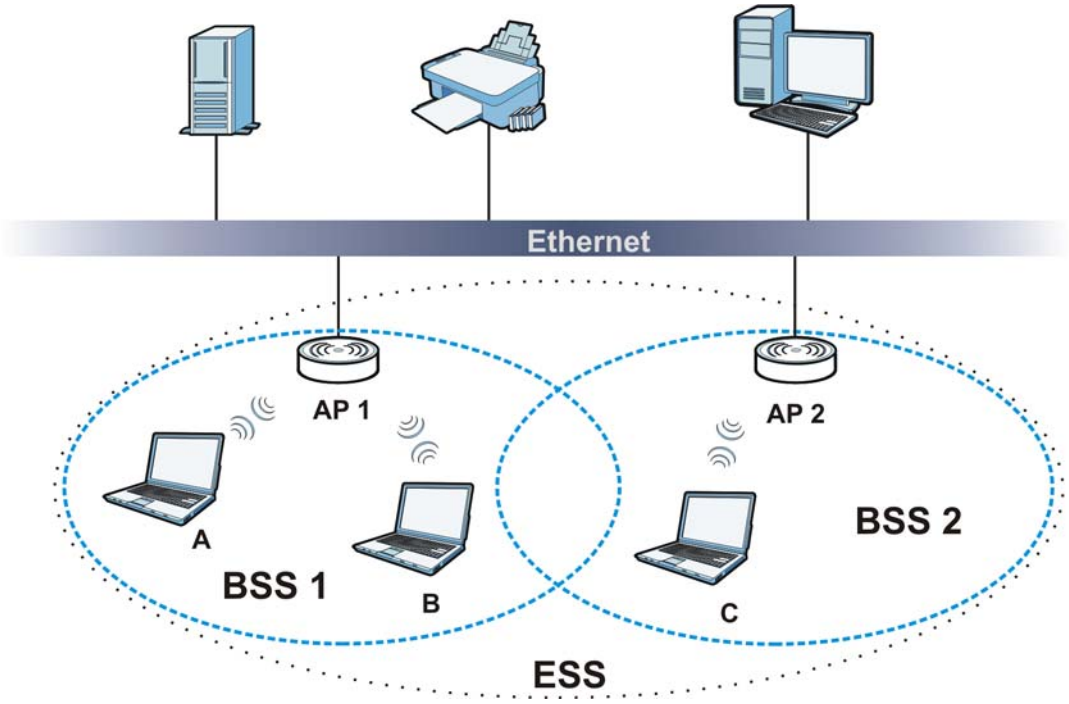
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 111 Infrastructure WLAN



Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

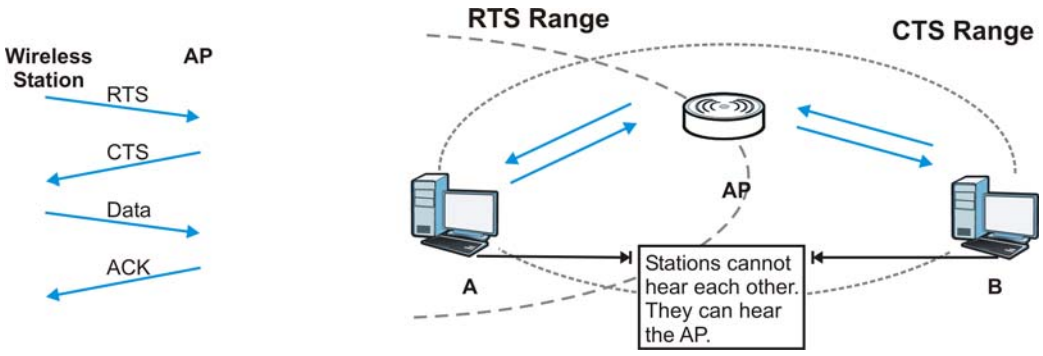
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a

hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 112 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the NWD2105 uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has

several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 28 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/ 48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the NWD2105 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the NWD2105 identity.

The following figure shows the relative effectiveness of these wireless security methods available on your NWD2105.

Table 29 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the NWD2105 and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.

- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.

- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 30 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption

keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

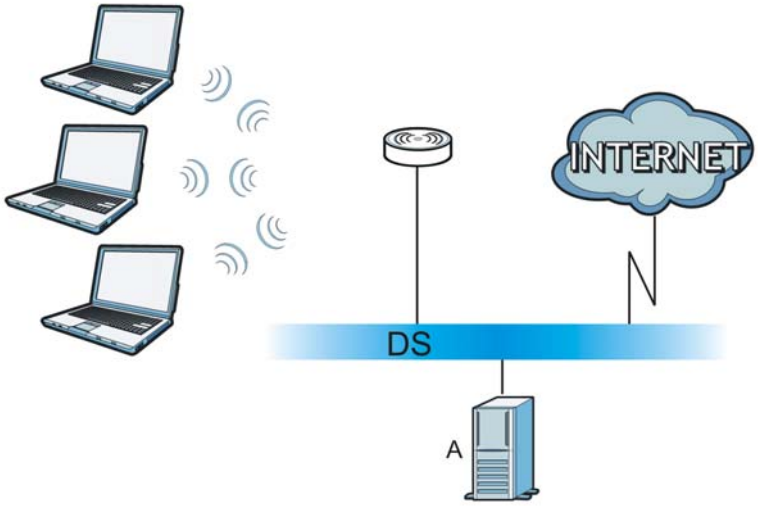
1 The AP passes the wireless client's authentication request to the RADIUS server.

2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.

4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 113 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

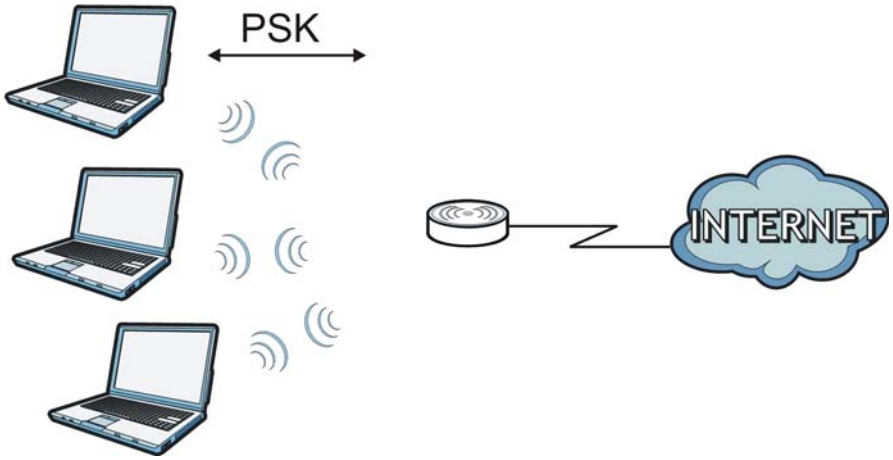
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

2 The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 114 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 31 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

C

Windows Wireless Management

This appendix shows you how to manage your NWD2105 using the Windows Vista and Windows XP wireless configuration tools.

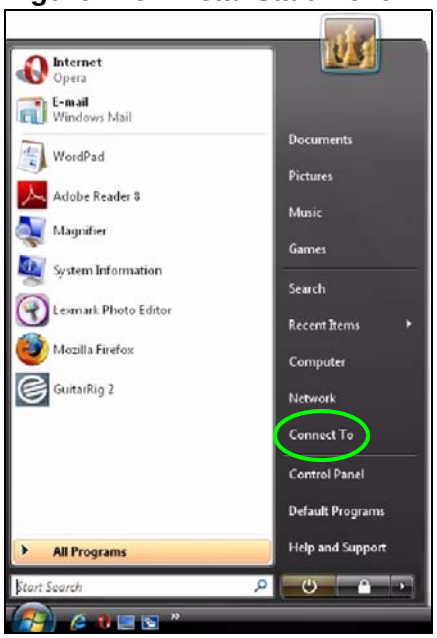
Windows Vista

Take the following steps to connect to a wireless network using the Windows Vista wireless configuration tool (WLAN AutoConfig).

Connecting to a Wireless Network

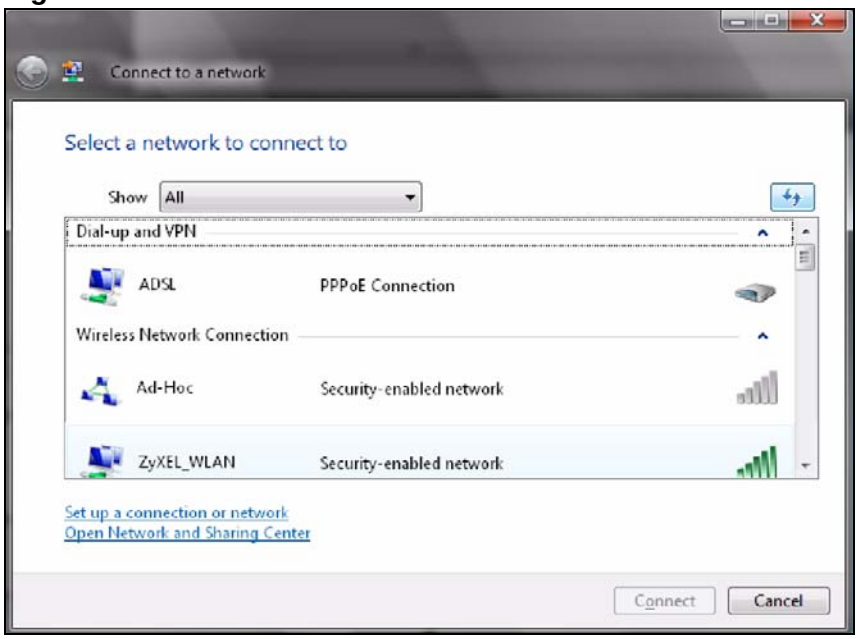
1 In the Windows Vista taskbar, click **Start** ( ) > **Connect To**.

Figure 115 Vista: Start Menu



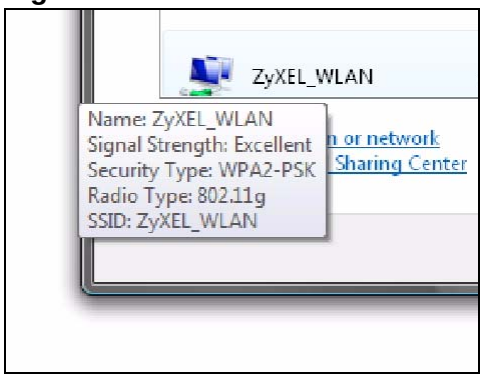
The **Connect To** window displays, showing all available networks.

Figure 116 Vista: The Connect To Window



The security status of each wireless network displays, as well as an indication of its signal strength. If you use the mouse pointer to hover over a network's entry, additional information about the network displays.

Figure 117 Vista: Additional Information

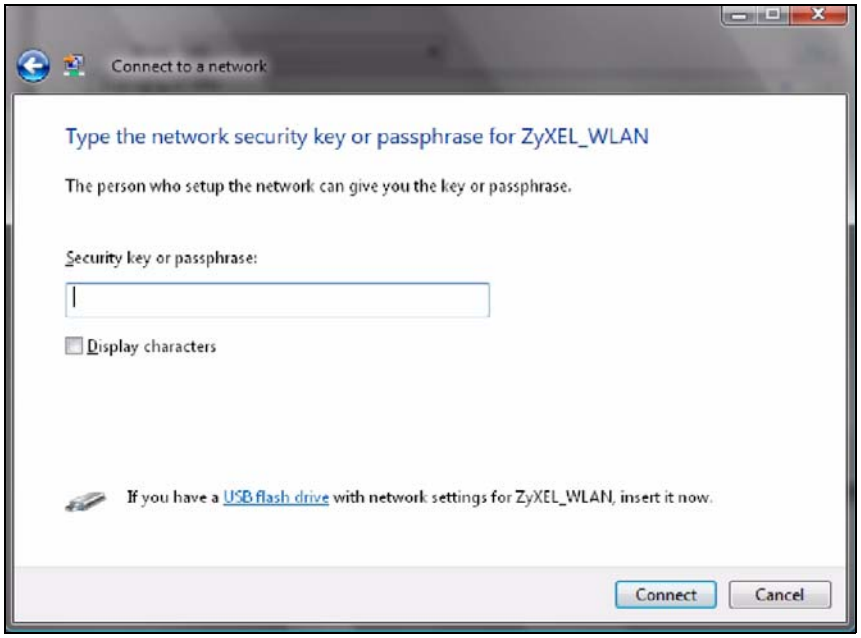


2 Double-click the network's name to join the network, or select a network and click **Connect**.

Note: If the network to which you want to connect does not display, see the section on setting up a connection manually on page 151.

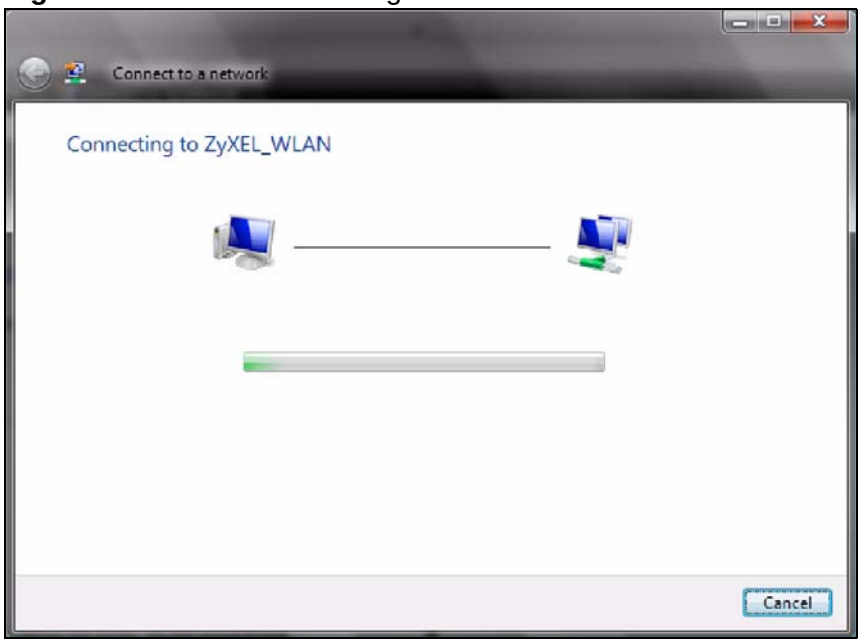
3 If security is enabled, you may be prompted to enter your security key.

Figure 118 Vista: Enter Security Key


Connect to a network
Type the network security key or passphrase for ZyXEL_WLAN
The person who setup the network can give you the key or passphrase.
Security key or passphrase:
Display characters
If you have a USB flash drive with network settings for ZyXEL_WLAN, insert it now.
Connect
Cancel

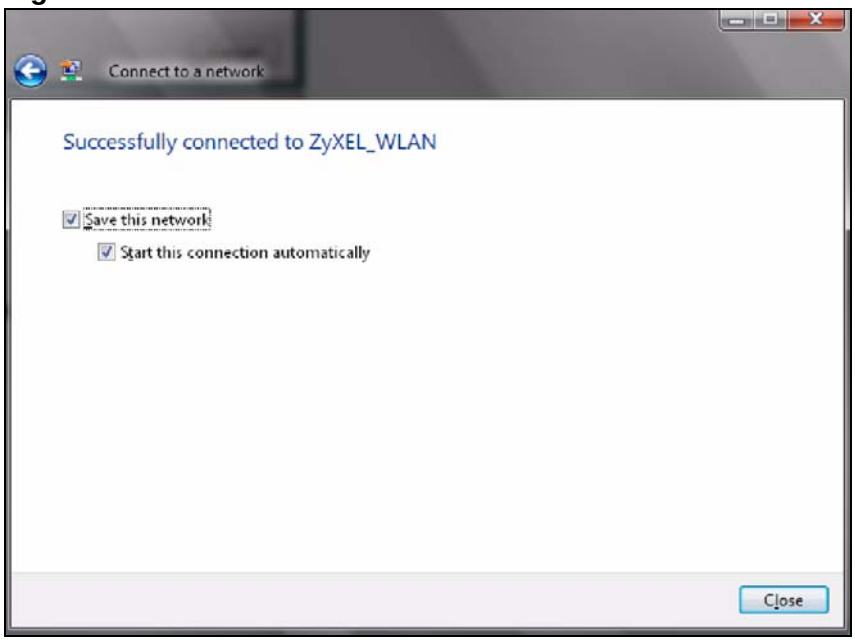
Your computer tries to connect to the wireless network.

Figure 119 Vista: Connecting



If your computer has connected to the wireless network successfully, the following screen displays.

Figure 120 Vista: Successful Connection



4 If you will use this network again, ensure that **Save this network** is selected. If you save the network, you do not have to configure its settings again.

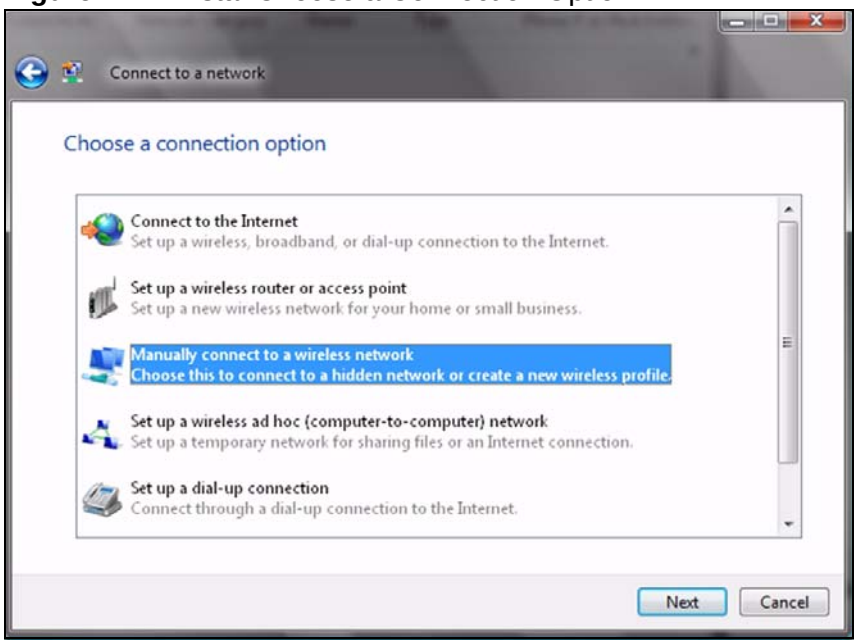
5 Select **Start this connection automatically** if you want Windows to always try to use this network when you start up your computer. If you do not select this (but select **Save this network**) you can connect manually each time by clicking **Start** > **Connect to** and selecting the network's name from the list.

Connecting to a Network Manually

If the wireless network to which you want to connect does not appear in the **Connect to** window (if your network's SSID is hidden, for example), take the following steps to configure your network connection manually

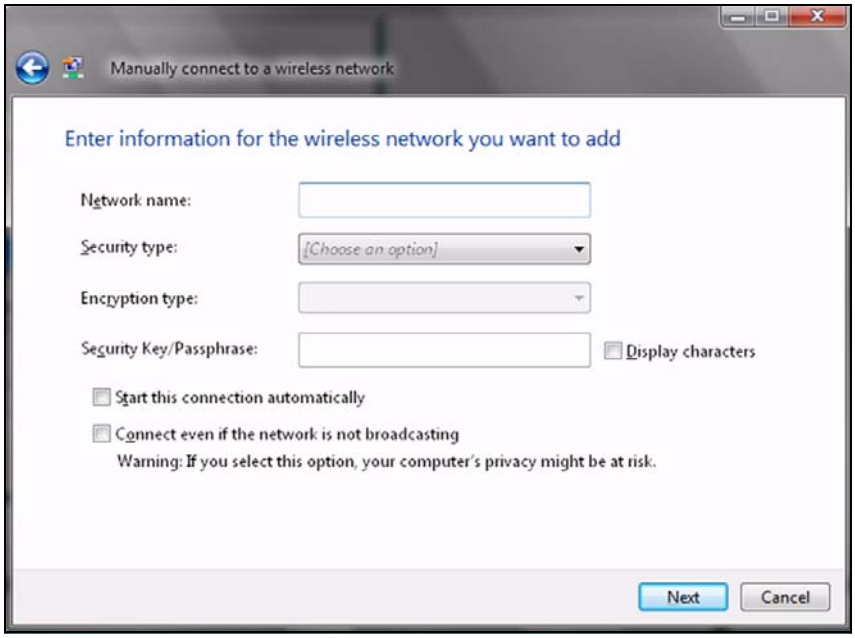
1 Click **Set up a connection or network** at the bottom of the **Connect to** screen. The following screen displays.

Figure 121 Vista: Choose a Connection Option


Connect to a network
Choose a connection option
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.
Set up a wireless router or access point
Set up a new wireless network for your home or small business.
Manually connect to a wireless network
Choose this to connect to a hidden network or create a new wireless profile.
Set up a wireless ad hoc (computer-to-computer) network
Set up a temporary network for sharing files or an Internet connection.
Set up a dial-up connection
Connect through a dial-up connection to the Internet.
Next
Cancel

2 Click **Manually connect to a wireless network**. The following screen displays.

Figure 122 Vista: Connect Manually


Manually connect to a wireless network
Enter information for the wireless network you want to add
Network name:
Security type:
[Choose an option]
Encryption type:
Security Key/Passphrase:
Display characters
Start this connection automatically
Connect even if the network is not broadcasting
Warning: If you select this option, your computer's privacy might be at risk.
Next
Cancel

The following table describes the labels in this screen.

Table 32 Vista: Connect Manually

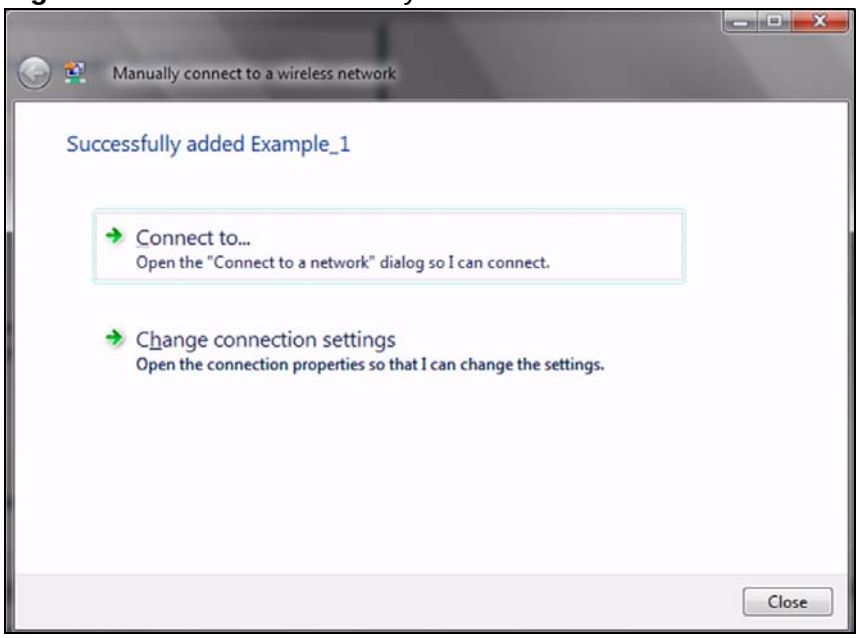
LABEL	DESCRIPTION
Network name	Enter your network's SSID (Service Set IDentifier).
Security type	Select the type of security used by the network to which you want to connect. The types of available security shown depend on your computer's wireless client. In this field, **WPA(2)-Personal** is the same as **WPA(2)-PSK**, and **WPA(2)-Enterprise** is the same as **WPA(2)**
Encryption type	Select the type of encryption used by the network. When you use **WEP** or **802.1x**, **WEP** displays. When you use a **WPA** mode (**WPA(2)-Personal** or **WPA(2)-Enterprise**) you can choose **AES** or **TKIP** (if supported by your computer's wireless client).
Security Key / Passphrase	If your network uses **WEP** or **WPA(2)-Personal** security, enter the key here.
Display Characters	Select this if you do not want the security key characters to be hidden.
Start this connection automatically	Select this box if you always want to try to connect to this network at startup. If you leave this box unchecked, you will need to connect manually each time.
Connect even if the network is not broadcasting	Select this box if you always want to try to connect to this network at startup, even if the network is not broadcasting its SSID. The warning in this field refers to the fact that if you do this, your computer sends out probe request packets, which contain the network's SSID and could be used by an attacker to access the network.

Table 32 Vista: Connect Manually

LABEL	DESCRIPTION
Next	Click this to save your settings and move on to the next page.
Cancel	Click this to stop setting up your network.

3 When you have finished filling in the fields, click **Next**. the following screen displays.

Figure 123 Vista: Successfully Added Network


Manually connect to a wireless network
Successfully added Example_1
Connect to...
Open the "Connect to a network" dialog so I can connect.
Change connection settings
Open the connection properties so that I can change the settings.
Close

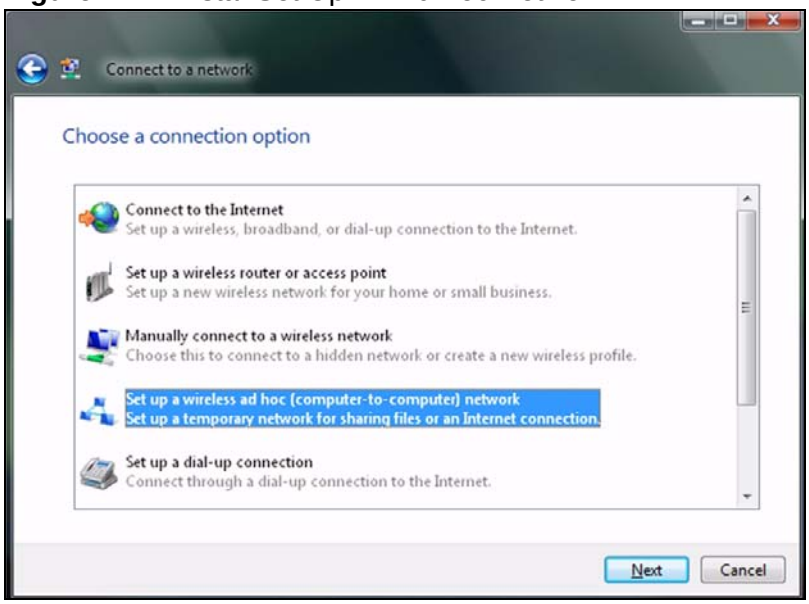
4 If you want to make any changes to the settings you just configured, click **Change connection settings**. Otherwise, click **Connect to...**. In the window that displays, double-click the new network's name to connect to the network.

Setting Up An Ad-Hoc Network

Take the following steps to set up a wireless connection between two computers in Windows Vista.

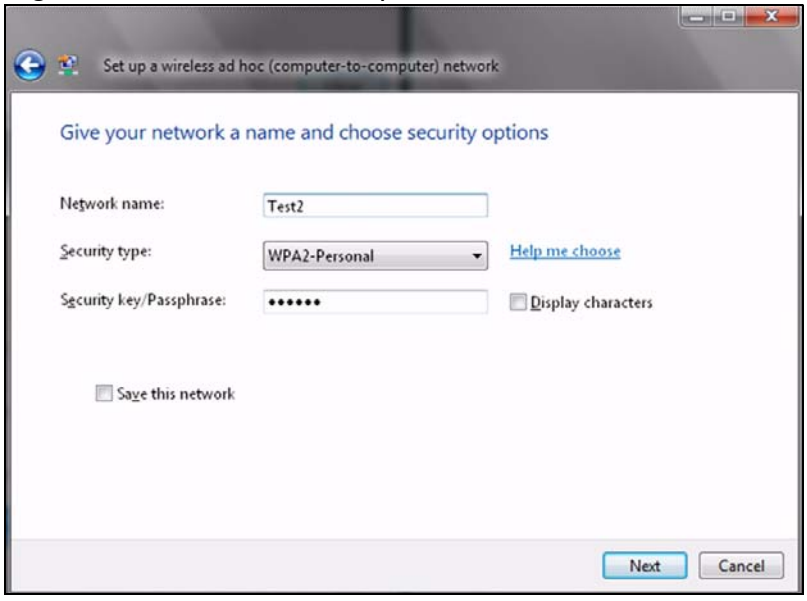
1 Click **Start** ( ) > **Connect To**. In the **Connect to** screen, click **Set up a connection or network**. The following screen displays.

Figure 124 Vista: Set Up An Ad-hoc Network


Connect to a network
Choose a connection option
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.
Set up a wireless router or access point
Set up a new wireless network for your home or small business.
Manually connect to a wireless network
Choose this to connect to a hidden network or create a new wireless profile.
Set up a wireless ad hoc (computer-to-computer) network
Set up a temporary network for sharing files or an Internet connection.
Set up a dial-up connection
Connect through a dial-up connection to the Internet.
Next
Cancel

2 Select **Set up a wireless ad hoc (computer-to-computer) network** and click **Next**. The following screen displays.

Figure 125 Vista: Ad-hoc Options



3 Enter the **Network name** (SSID) you want to use for your network. Select a **Security type**. If you are not sure what kind of security you want to use, click the **Help me choose** link.

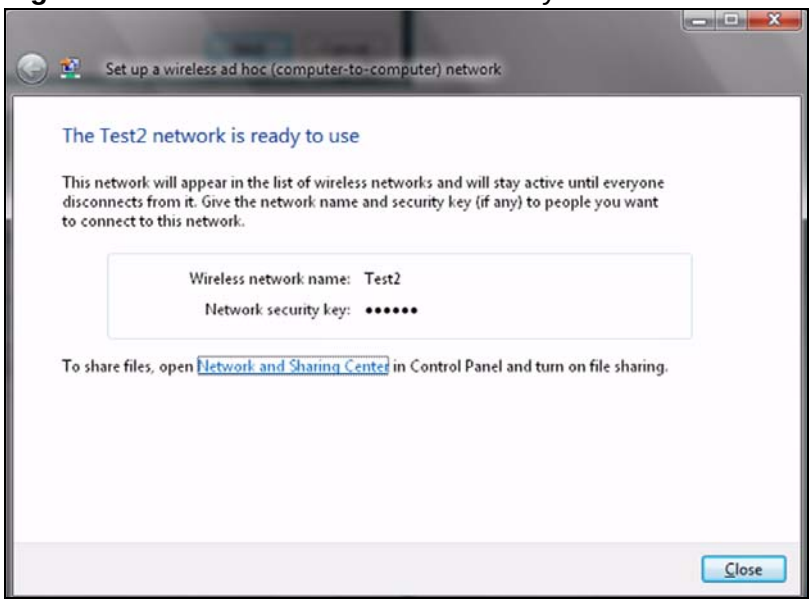
Note: Make sure all the wireless clients on your ad-hoc network can support the type of security you select.

4 Enter the **Security key/Passphrase**. Everybody on the network must enter this key in their computer's wireless client in order to access the network. If you want to see the characters you entered, select the **Display characters** box. Otherwise, leave it empty (dots display instead of the characters).

5 If you will use this ad-hoc network again, select the **Save this network** box. If you do this, the next time you click **Start** > **Connect to**, you can select the network from the list.

6 Click **Next**. The following screen displays.

Figure 126 Vista: Ad-hoc Network Ready


Set up a wireless ad hoc (computer-to-computer) network
The Test2 network is ready to use
This network will appear in the list of wireless networks and will stay active until everyone disconnects from it. Give the network name and security key (if any) to people you want to connect to this network.
Wireless network name: Test2
Network security key: ••••••
To share files, open Network and Sharing Center in Control Panel and turn on file sharing.
Close

7 If you want to share files with other computers on the ad-hoc network, or let other computers use your Internet connection, click the **Network and Sharing Center** link. Otherwise, click **Close**.

Windows XP

Be sure you have the Windows XP service pack 2 installed on your computer. Otherwise, you should at least have the Windows XP service pack 1 already on your computer and download the support patch for WPA from the Microsoft web site.

Windows XP SP2 screen shots are shown unless otherwise specified. Click the help icon ( ) in most screens, move the cursor to the item that you want the information about and click to view the help.

Activating Wireless Zero Configuration

1 Click **Start**, **Control Panel** and double-click **Network Connections**.

2 Double-click on the icon for wireless network connection.

3 The status window displays as shown below. Click **Properties**.

Figure 127 Windows XP SP1: Wireless Network Connection Status

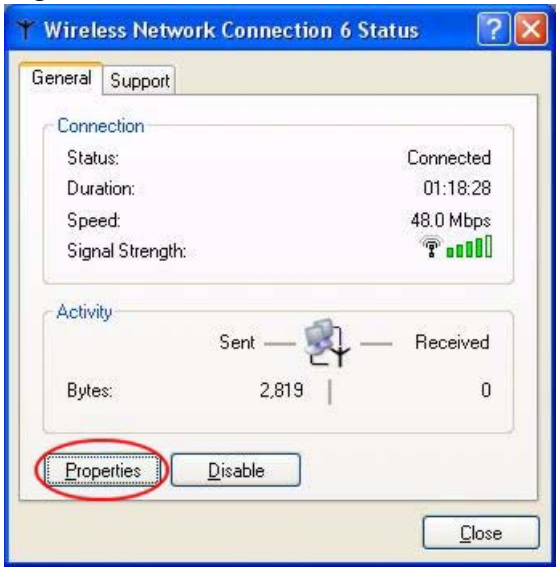
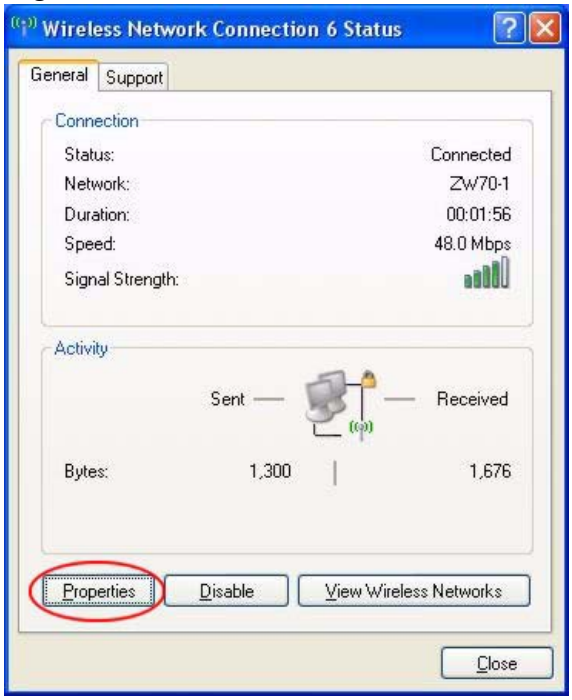


Figure 128 Windows XP SP2: Wireless Network Connection Status



4 The **Wireless Network Connection Properties** screen displays. Click the **Wireless Networks** tab.

Make sure the **Use Windows to configure my wireless network settings** check box is selected.

Figure 129 Windows XP SP1: Wireless Network Connection Properties

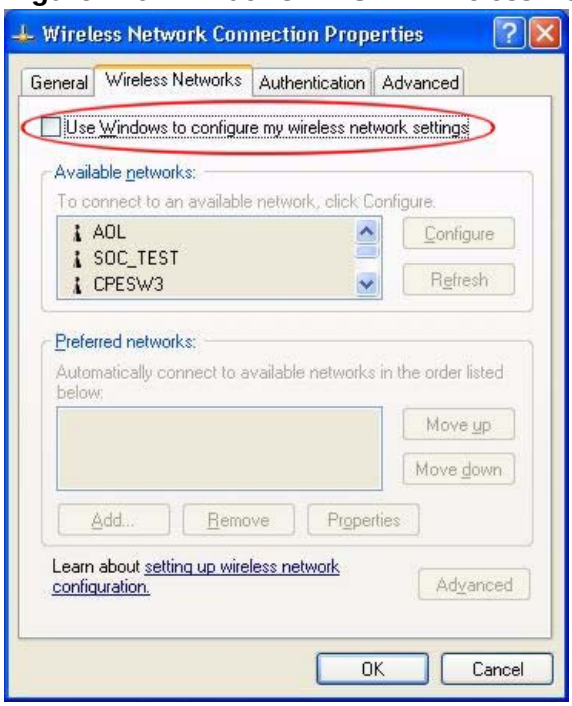
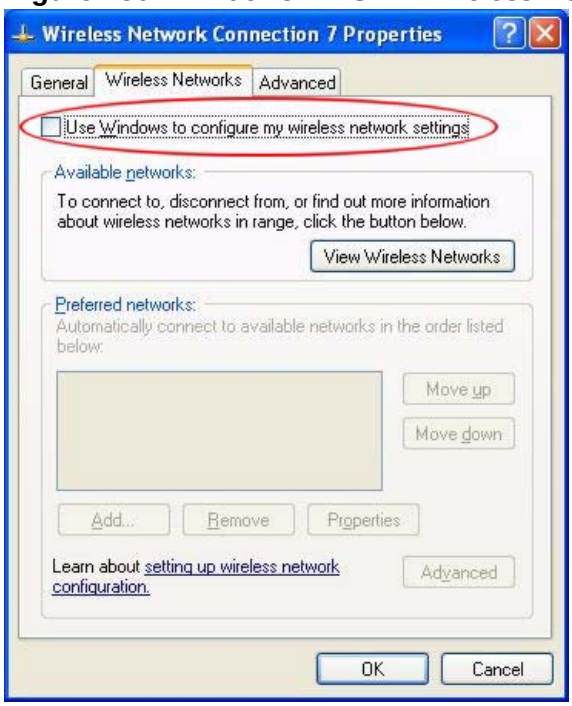
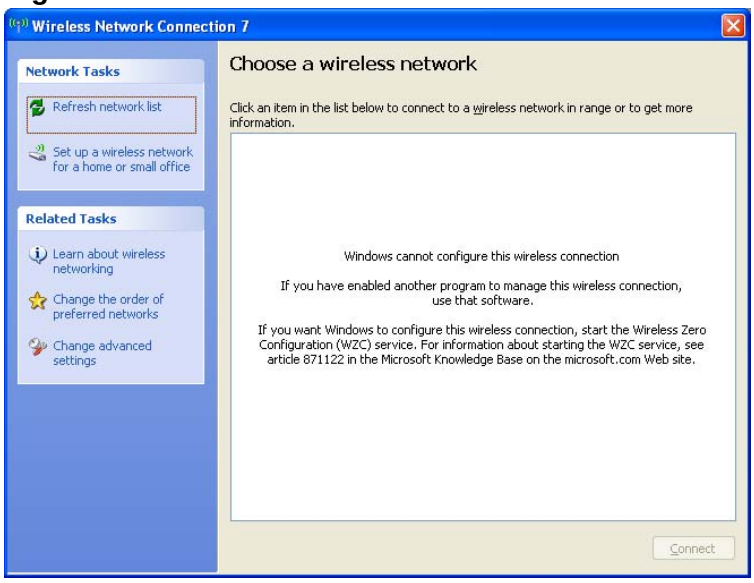


Figure 130 Windows XP SP2: Wireless Network Connection Properties



If you see the following screen, refer to article 871122 on the Microsoft web site for information on starting WZC.

Figure 131 Windows XP SP2: WZC Not Available


Wireless Network Connection 7
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
Windows cannot configure this wireless connection
If you have enabled another program to manage this wireless connection, use that software.
If you want Windows to configure this wireless connection, start the Wireless Zero Configuration (WZC) service. For information about starting the WZC service, see article 871122 in the Microsoft Knowledge Base on the microsoft.com Web site.
Connect

Connecting to a Wireless Network

1 Double-click the network icon for wireless connections in the system tray to open the Wireless Network Connection Status screen.

Figure 132 Windows XP SP2: System Tray Icon

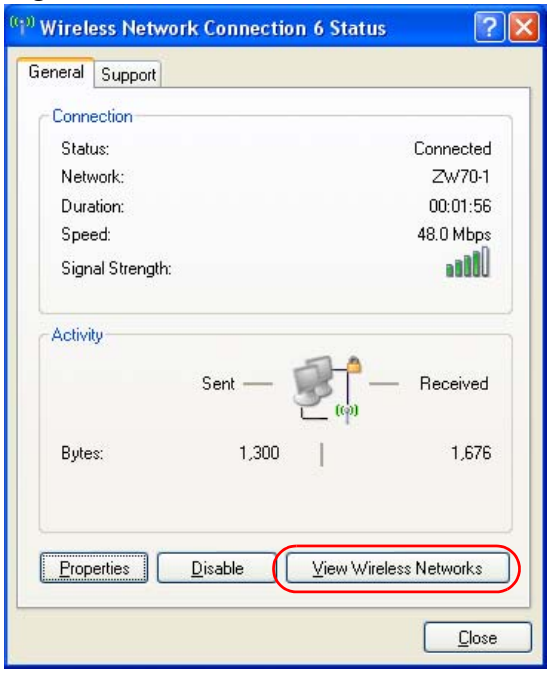
The type of the wireless network icon in Windows XP SP2 indicates the status of the NWD2105. Refer to the following table for details.

Table 33 Windows XP SP2: System Tray Icon

ICON	DESCRIPTION
	The NWD2105 is connected to a wireless network.
	The NWD2105 is in the process of connecting to a wireless network.
	The connection to a wireless network is limited because the network did not assign a network address to the computer.
	The NWD2105 is not connected to a wireless network.

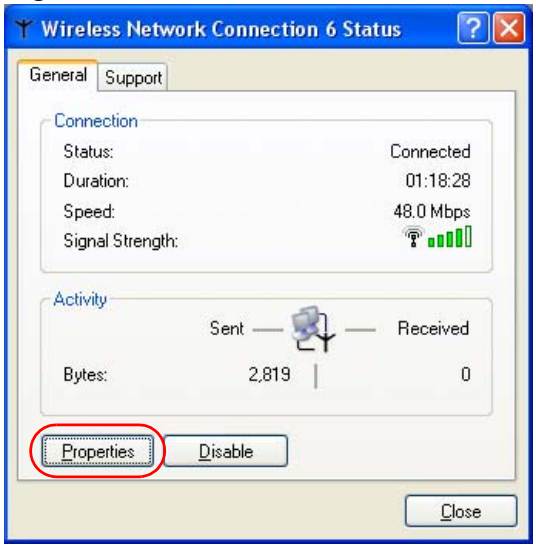
2 Windows XP SP2: In the **Wireless Network Connection Status** screen, click **View Wireless Networks** to open the **Wireless Network Connection** screen.

Figure 133 Windows XP SP2: Wireless Network Connection Status



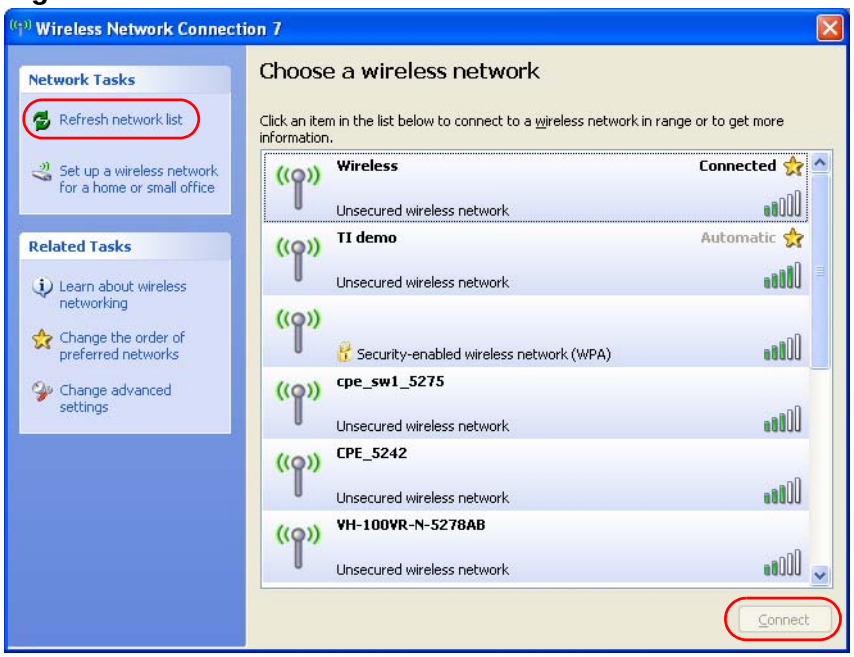
Windows XP SP1: In the **Wireless Network Connection Status** screen, click **Properties** and the **Wireless Networks** tab to open the **Wireless Network Connection Properties** screen.

Figure 134 Windows XP SP1: Wireless Network Connection Status



3 Windows XP SP2: Click **Refresh network list** to reload and search for available wireless devices within transmission range. Select a wireless network in the list and click **Connect** to join the selected wireless network.

Figure 135 Windows XP SP2: Wireless Network Connection



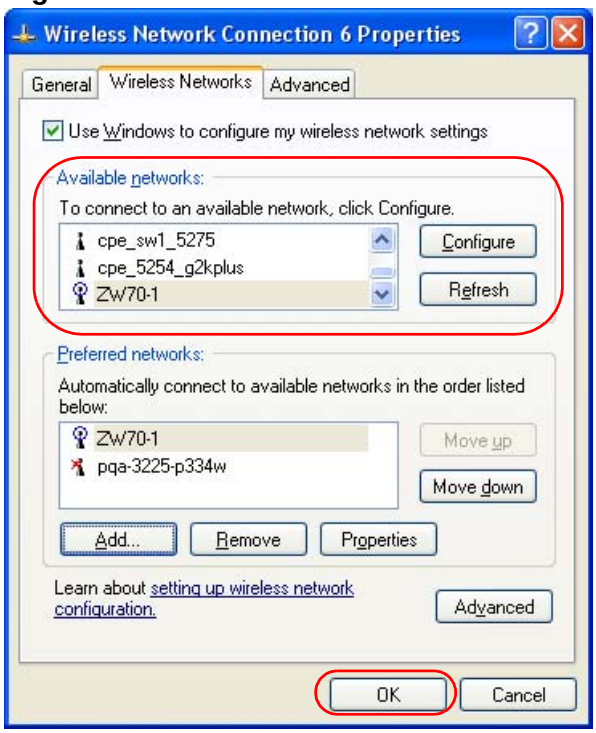
The following table describes the icons in the wireless network list.

Table 34 Windows XP SP2: Wireless Network Connection

ICON	DESCRIPTION
	This denotes that wireless security is activated for the wireless network.
	This denotes that this wireless network is your preferred network. Ordering your preferred networks is important because the NWD2105 tries to associate to the preferred network first in the order that you specify. Refer to the section on ordering the preferred networks for detailed information.
	This denotes the signal strength of the wireless network. Move your cursor to the icon to see details on the signal strength.

Windows XP SP1: Click **Refresh** to reload and search for available wireless devices within transmission range. Select a wireless network in the **Available networks** list, click **Configure** and set the related fields to the same security settings as the associated AP to add the selected network into the **Preferred** networks table. Click **OK** to join the selected wireless network. Refer to the section on security settings (discussed later) for more information.

Figure 136 Windows XP SP1: Wireless Network Connection Properties



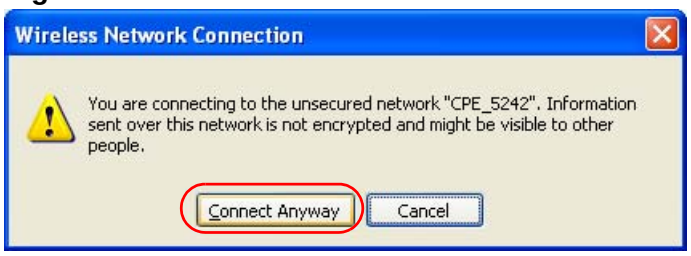
4 4.Windows XP SP2: If the wireless security is activated for the selected wireless network, the **Wireless Network Connection** screen displays. You must set the related fields in the **Wireless Network Connection** screen to the same security settings as the associated AP and click **Connect**. Refer to the section about

security settings for more information. Otherwise click **Cancel** and connect to another wireless network without data encryption. If there is no security activated for the selected wireless network, a warning screen appears. Click **Connect Anyway** if wireless security is not your concern.

Figure 137 Windows XP SP2: Wireless Network Connection: WEP or WPA-PSK

Wireless Network Connection
The network 'cpe_5236' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.
Type the key, and then click Connect.
Network key:
Confirm network key:
Connect
Cancel

Figure 138 Windows XP SP2: Wireless Network Connection: No Security


Wireless Network Connection
You are connecting to the unsecured network "CPE_5242". Information sent over this network is not encrypted and might be visible to other people.
Connect Anyway
Cancel

5 Verify that you have successfully connected to the selected network and check the connection status in the wireless network list or the connection icon in the **Preferred networks** or **Available networks** list.

The following table describes the connection icons.

Table 35 Windows XP: Wireless Networks

ICON	DESCRIPTION
	This denotes the wireless network is an available wireless network.
	This denotes the NWD2105 is associated to the wireless network.
	This denotes the wireless network is not available.

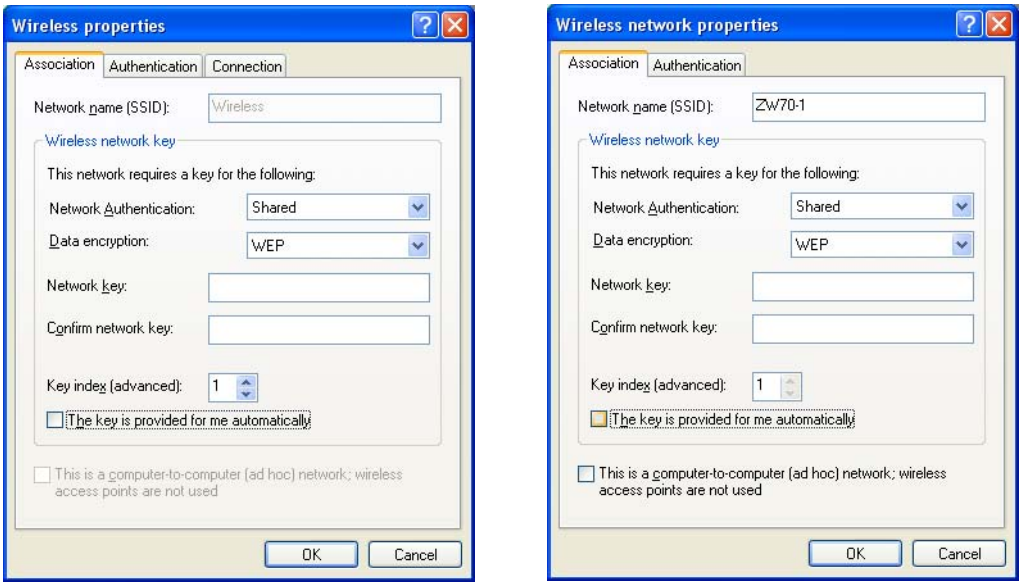
Security Settings

When you configure the NWD2105 to connect to a secure network but the security settings are not yet enabled on the NWD2105, you will see different screens according to the authentication and encryption methods used by the selected network.

Association

Select a network in the Preferred networks list and click Properties to view or configure security.

Figure 139 Windows XP: Wireless (network) properties: Association



The following table describes the labels in this screen.

Table 36 Windows XP: Wireless (network) properties: Association

LABEL	DESCRIPTION
Network name (SSID)	This field displays the SSID (Service Set IDentifier) of each wireless network.
Network Authentication	This field automatically shows the authentication method (**Share**, **Open**, **WPA** or **WPA-PSK**) used by the selected network.
Data Encryption	This field automatically shows the encryption type (**TKIP**, **WEP** or **Disable**) used by the selected network.
Network Key	Enter the pre-shared key or WEP key. The values for the keys must be set up exactly the same on all wireless devices in the same wireless LAN.
Confirm network key	Enter the key again for confirmation.
Key index (advanced)	Select a default WEP key to use for data encryption. This field is available only when the network use **WEP** encryption method and the **The key is provided for me automatically** check box is not selected.
The key is provided for me automatically	If this check box is selected, the wireless AP assigns the NWD2105 a key.

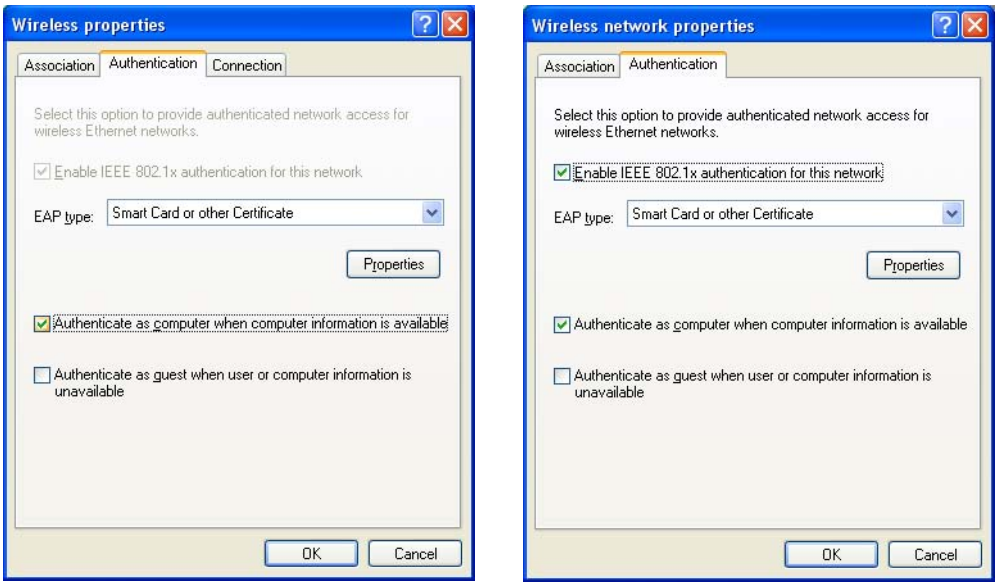
Table 36 Windows XP: Wireless (network) properties: Association (continued)

LABEL	DESCRIPTION
This is a computer-to-computer (ad hoc) network; wireless access points are not used	If this check box is selected, you are connecting to another computer directly.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to leave this screen without saving any changes you may have made.

Authentication

Click the **Authentication** tab in the **Wireless (network) properties** screen to display the screen shown next. The fields on this screen are grayed out when the network is in Ad-Hoc mode or data encryption is disabled.

Figure 140 Windows XP: Wireless (network) properties: Authentication


Wireless properties
Association
Authentication
Connection
Select this option to provide authenticated network access for wireless Ethernet networks.
Enable IEEE 802.1x authentication for this network
EAP type:
Smart Card or other Certificate
Properties
Authenticate as computer when computer information is available
Authenticate as guest when user or computer information is unavailable
OK
Cancel
Wireless network properties
Association
Authentication
Select this option to provide authenticated network access for wireless Ethernet networks.
Enable IEEE 802.1x authentication for this network
EAP type:
Smart Card or other Certificate
Properties
Authenticate as computer when computer information is available
Authenticate as guest when user or computer information is unavailable
OK
Cancel

The following table describes the labels in this screen.

Table 37 Windows XP: Wireless (network) properties: Authentication

LABEL	DESCRIPTION
Enable IEEE 802.1x authentication for this network	This field displays whether the IEEE 802.1x authentication is active. If the network authentication is set to **Open** in the previous screen, you can choose to disable or enable this feature.
EAP Type	Select the type of EAP authentication. Options are **Protected EAP (PEAP)** and **Smart Card or other Certificate**.

Table 37 Windows XP: Wireless (network) properties: Authentication (continued)

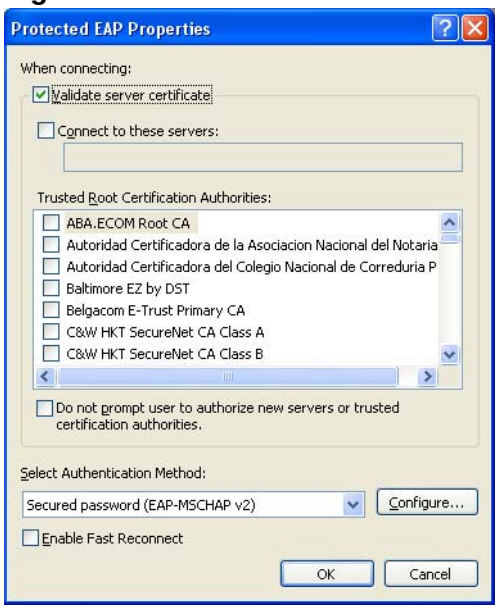
LABEL	DESCRIPTION
Properties	Click this button to open the properties screen and configure certificates. The screen varies depending on what you select in the **EAP type** field.
Authenticate as computer when computer information is available	Select this check box to have the computer send its information to the network for authentication when a user is not logged on.
Authenticate as guest when user or computer information is unavailable	Select this check box to have the computer access to the network as a guest when a user is not logged on or computer information is not available.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to leave this screen without saving any changes you may have made.

Authentication Properties

Select an EAP authentication type in the **Wireless (network) properties: Authentication** screen and click the **Properties** button to display the following screen.

Protected EAP Properties

Figure 141 Windows XP: Protected EAP Properties


Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
ABA.ECOM Root CA
Autoridad Certificadora de la Asociacion Nacional del Notaria
Autoridad Certificadora del Colegio Nacional de Correduria P
Baltimore EZ by DST
Belgacom E-Trust Primary CA
C&W HKT SecureNet CA Class A
C&W HKT SecureNet CA Class B
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
OK
Cancel

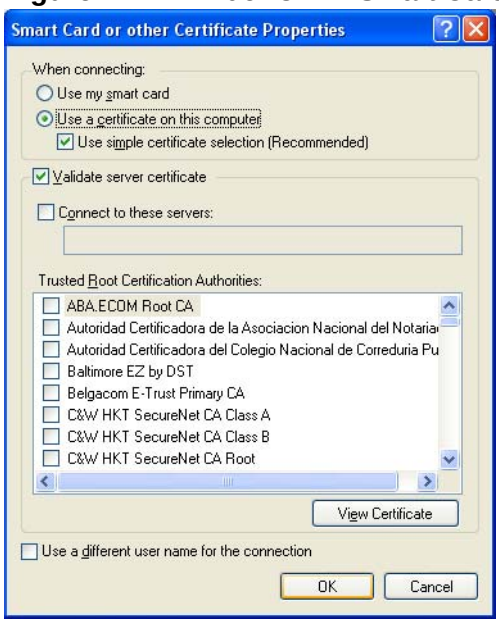
The following table describes the labels in this screen.

Table 38 Windows XP: Protected EAP Properties

LABEL	DESCRIPTION
Validate server certificate	Select the check box to verify the certificate of the authentication server.
Connect to these servers	Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain.
Trusted Root Certification Authorities:	Select a trusted certification authority from the list below. Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.
Do not prompt user to authorize new server or trusted certification authorities.	Select this check box to verify a new authentication server or trusted CA without prompting. This field is available only if you installed the Windows XP server pack 2.
Select Authentication Method:	Select an authentication method from the drop-down list box and click **Configure** to do settings.
Enable Fast Reconnect	Select the check box to automatically reconnect to the network (without re-authentication) if the wireless connection goes down.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to leave this screen without saving any changes you may have made.

Smart Card or other Certificate Properties

Figure 142 Windows XP: Smart Card or other Certificate Properties


Smart Card or other Certificate Properties
When connecting:
Use my smart card
Use a certificate on this computer
Use simple certificate selection (Recommended)
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
ABA.ECOM Root CA
Autoridad Certificadora de la Asociacion Nacional del Notariat
Autoridad Certificadora del Colegio Nacional de Correduria Pu
Baltimore EZ by DST
Belgacom E-Trust Primary CA
C&W HKT SecureNet CA Class A
C&W HKT SecureNet CA Class B
C&W HKT SecureNet CA Root
View Certificate
Use a different user name for the connection
OK
Cancel

The following table describes the labels in this screen.

Table 39 Windows XP: Smart Card or other Certificate Properties

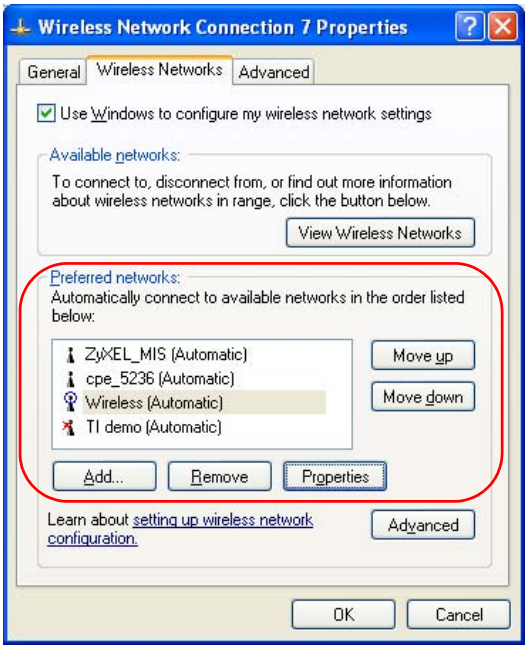
LABEL	DESCRIPTION
Use my smart card	Select this check box to use the smart card for authentication.
Use a certificate on this computer	Select this check box to use a certificate on your computer for authentication.
Validate server certificate	Select the check box to check the certificate of the authentication server.
Connect to these servers	Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain.
Trusted Root Certification Authorities:	Select a trusted certification authority from the list below. Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.
View Certificate	Click this button if you want to verify the selected certificate.
Use a different user name for the connection:	Select the check box to use a different user name when the user name in the smart card or certificate is not the same as the user name in the domain that you are logged on to.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to leave this screen without saving any changes you may have made.

Ordering the Preferred Networks

Follow the steps below to manage your preferred networks.

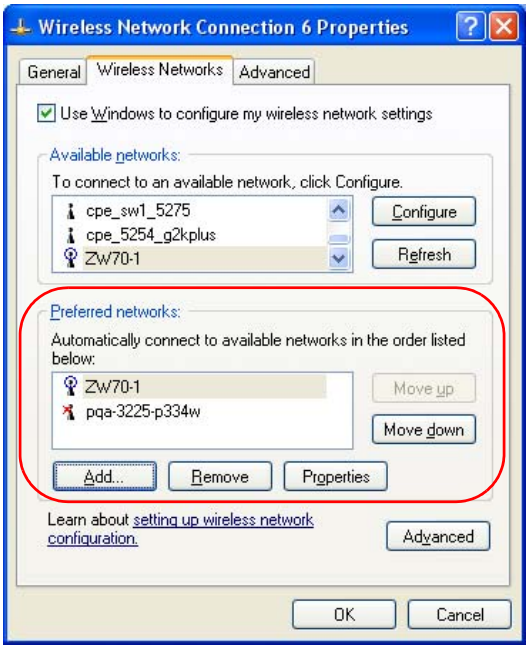
1 Windows XP SP2: Click **Change the order of preferred networks** in the **Wireless Network Connection** screen (see Figure 135 on page 161). The screen displays as shown.

Figure 143 Windows XP SP2: Wireless Networks: Preferred Networks



Windows XP SP1: In the **Wireless Network Connection Status** screen, click **Properties** and the **Wireless Networks** tab to open the screen as shown.

Figure 144 Windows XP SP1: Wireless Networks: Preferred Networks



2 Whenever the NWD2105 tries to connect to a new network, the new network is added in the **Preferred networks** table automatically. Select a network and click **Move up** or **Move down** to change it's order, click **Remove** to delete it or click **Properties** to view the security, authentication or connection information of the selected network. Click **Add** to add a preferred network into the list manually.

D

Wireless for Windows 7

Follow these steps to connect to a wireless network for a computer with the Windows 7 Operating System (OS).

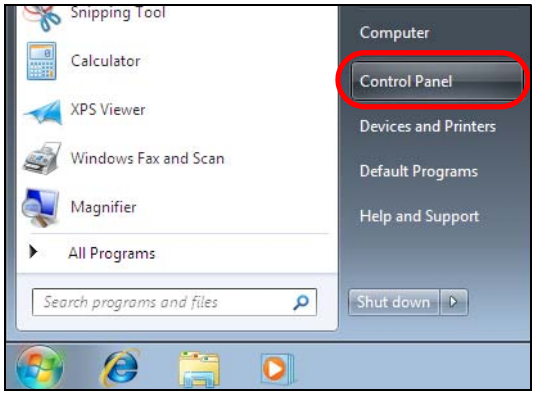
You should know the network name (SSID) of the wireless network to which you want to connect. You should also know the password (pre-shared key (PSK)/ passphrase) if the wireless network is secured.

Enabling the Wireless Adapter

Do the following to enable the wireless adapter of your computer. If you know for a fact that the wireless adapter is already working, you can skip this part and go to Connecting to a Wireless Network.

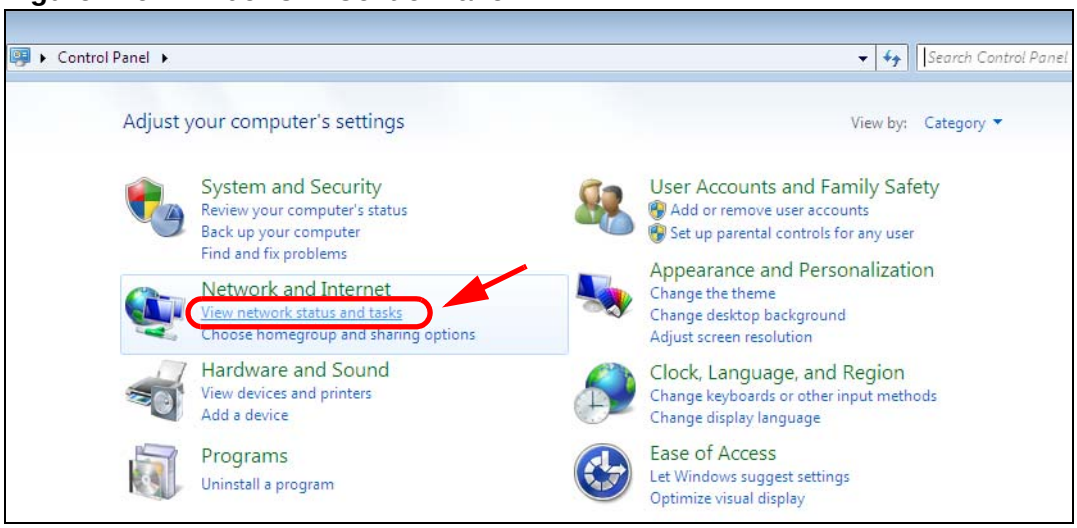
1 Click **Start** > **Control Panel**.

Figure 145 Windows 7: Start Menu



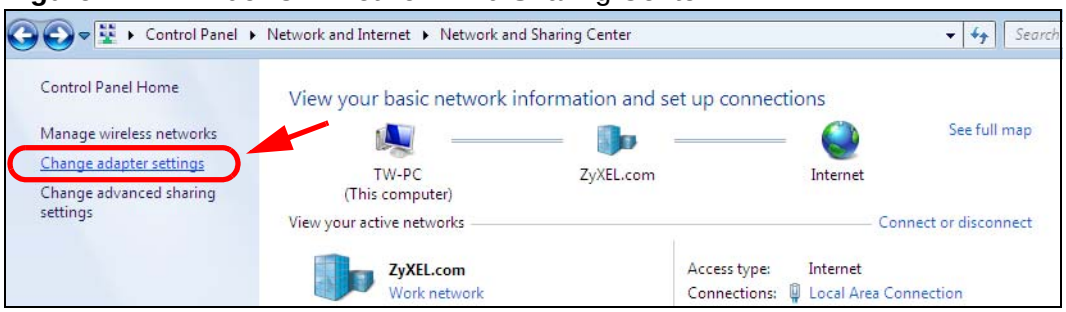
2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

Figure 146 Windows 7: Control Panel



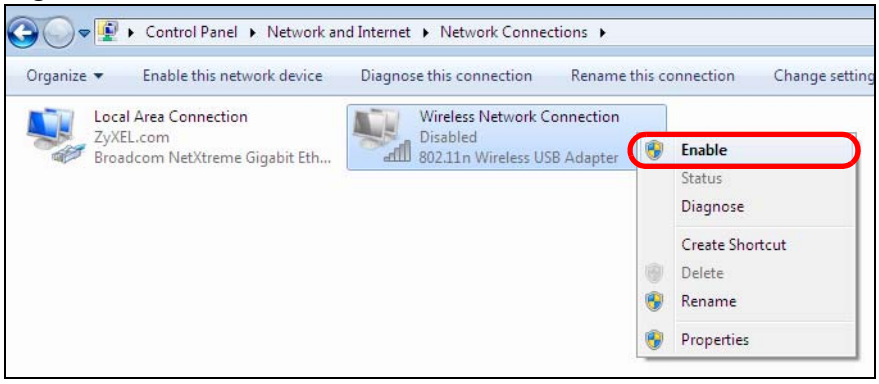
3 Click **Change adapter settings**.

Figure 147 Windows 7: Network And Sharing Center



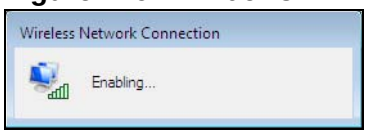
4 Right click **Wireless Network Connection** and select **Enable**.

Figure 148 Windows 7: Wireless Network Connection



A progress indicator appears.

Figure 149 Windows 7: Enabling the Wireless Network Connection



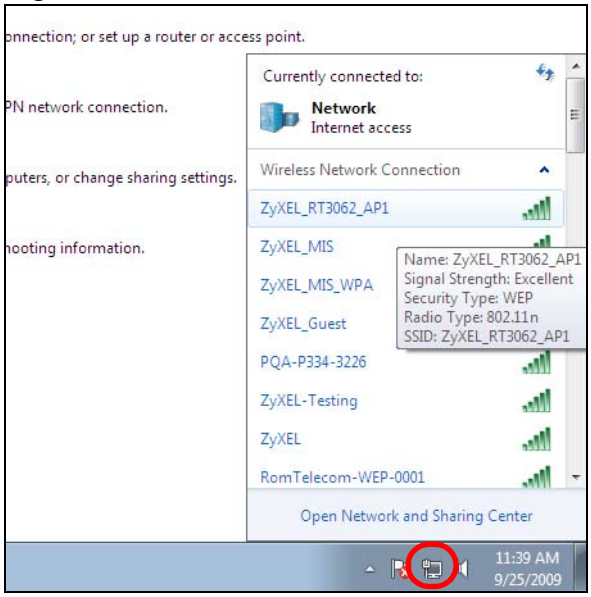
When it shows **Enabled**, you are ready to connect to your wireless network.

Connecting to a Wireless Network

Once the computer's wireless adapter has been enabled, do the following to connect to a wireless network.

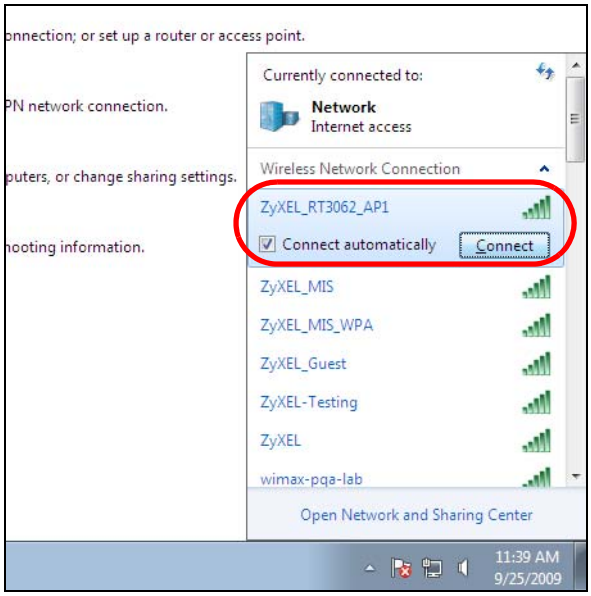
1 Click the wireless adapter icon which appears in the bottom right of your computer monitor. A list of available wireless networks displays.

Figure 150 Windows 7: List of Wireless Networks



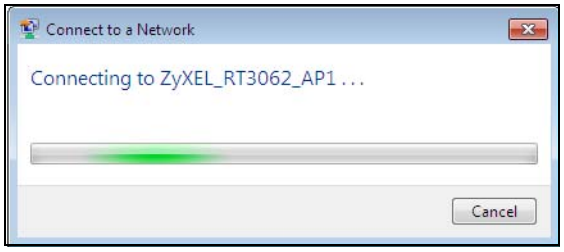
2 Select a wireless network and click **Connect**.

Figure 151 Windows 7: Connect to the Wireless Networks



- If the wireless network is not password-protected, you should see a progress indicator as follows.

Figure 152 Windows 7: Wireless Connection Progress Indicator



- If the wireless network is secured, you should provide the correct credentials before you can gain access as shown below.

Figure 153 Windows 7: Wireless Connection Security

You may have to wait several minutes while your computer connects to the wireless network.

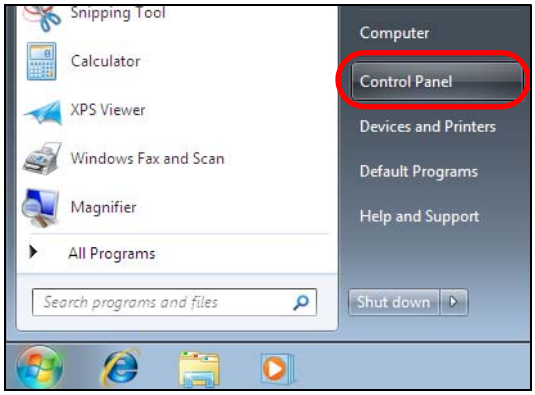
Verifying the Settings

Open a web browser and try to access a website, such as www.zyxel.com.

Additionally, do the following to check your wireless network connection status.

1 Click **Start** > **Control Panel**.

Figure 154 Windows 7: Start Menu

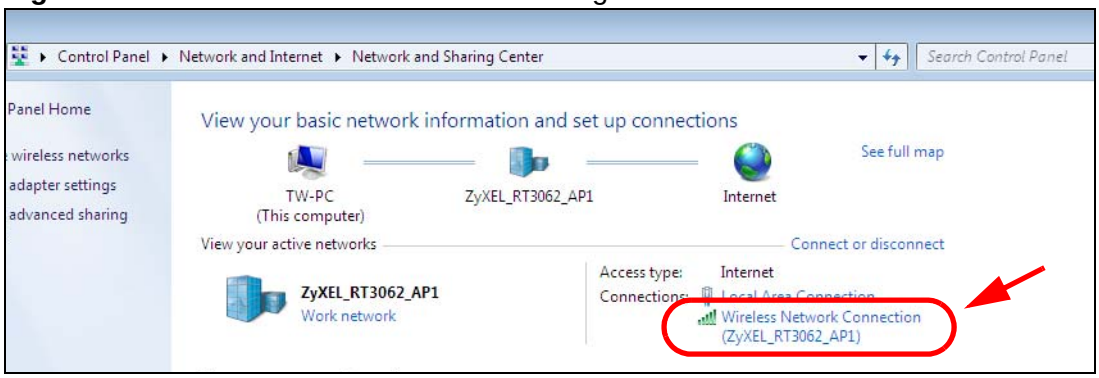


2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

Figure 155 Windows 7: Control Panel

3 Check the **Connections** under **View you active networks**. If the wireless network name displays and the icon is green, you have successfully connected to the wireless network.

Figure 156 Windows 7: Network and Sharing Center



E

Legal Information

Copyright

Copyright © 2010 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This device has been tested to the FCC exposure requirements (Specific Absorption Rate).
- This device complies with the requirements of Health Canada Safety Code 6 for Canada.
- Testing was performed on laptop computers with antennas at 5mm spacing. The maximum SAR value is: 0.77 W/kg. The device must not be collocated with any other antennas or transmitters.
- This equipment has been SAR-evaluated for use in laptops (notebooks) with side slot configuration.
- The device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2). End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

1) this device may not cause interference and

2) this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 3dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IC Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

注意 !

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index

A

About 86
about your ZyXEL Device 18
Access Point (AP) 38
Access point (AP) 38
Access Point. See also AP.
ACT LED 19
activating a profile 67
adapter 68
Ad-Hoc 20, 65
Advanced Encryption Standard 41
  See AES.
advanced settings 68
AES 141
antenna
  directional 146
  gain 145
  omni-directional 146
Antenna gain 80
Antenna output power 78
AP
  See also access point.
AP (access point) 133
AP MAC address 52
AP mode
  configuration 34
Association list 35, 78
authentication 52
authentication type 40
  auto 40
  open system 40
  shared key 40
auto authentication 40
automatic connection 54
automatic network scan 29, 62

B

Basic Service Set, See BSS 131
BSS 131

C

CA 41, 139
CCMP 41
Certificate Authority
  See CA.
certifications 179
  notices 181
  viewing 182
channel 39, 52, 54, 55, 65, 79, 133
  interference 133
configuration method 21
  important note 21
  Wireless Zero Configuration (WZC) 20, 21
  ZyXEL utility 21
configuration status 51, 78
connection status 51, 78
copyright 179
creating a new profile 64
credentials 72
CTS (Clear to Send) 134
current configuration 51, 78
current connection status 51, 78

D

data encryption 55
digital ID 41
dimensions 95
disclaimer 179
download 87
driver version 86

dynamic WEP key exchange 140

E

EAP (Extensible Authentication Protocol) 40
EAP Authentication 138
EAP authentication 41
EAP type 71
EAP-PEAP 40
EAP-TLS 40
EAP-TTLS 40
encryption 141
encryption type 40, 59
environmental specifications 95
ESS 132
Extended Service Set, See ESS 132

F

FCC interference statement 179
fragmentation threshold 135
frequency 39, 96

G

getting started 17

H

hardware connections 20
help 22
hidden node 133
humidity 95

I

IBSS 131
IEEE 802.11g 135
IEEE 802.1x 40, 59, 71
Independent Basic Service Set
  See IBSS 131
infrastructure 19
initialization vector (IV) 141
installation 20
interface 95
Internet access 19
IP address
  dynamic 77

L

LEDs 19
lights 19
link information 51, 78
LINK LED 19
link quality 52

M

MAC 78
MAC filter 83
  action 84
manual network connection 29
Mbps 78
Message Integrity Check (MIC) 41, 141

N

Network interface card (NIC) 80
network mode 52
network name 52
network overlap 39
network scan 62
Network sharing 77
network type 52, 55

O

online help 22
Output power 78

P

packet collisions 52
Pairwise Master Key (PMK) 141, 143
passphrase 40, 56, 81
password 40
PEAP 71, 72
peer computer 19, 65
physical specifications 95
power saving mode 68
preamble mode 135
product registration 183
product specifications 95
Profile 62
profile 51, 63
  activation 67
  add new 64
  configure 29, 31
  default 62
  delete 63
  edit 63
  information 63
  new 63, 64
PSK 141

Q

Quick Start Guide 20, 92

R

radio interference 92
radio specifications 95, 96
RADIUS 40, 41, 137
  message types 137
  messages 137
  shared secret key 138
real-time data traffic statistics 53
receive rate 52
receive speed 52
registration
  product 183
related documentation 3
RTS (Request To Send) 134
  threshold 133, 134

S

safety warnings 7
Save power 80
save power 68
scan 54
scan info 65
search 54
Security 78
security 39, 52, 97
  data encryption 39
security settings and Vista 71
sensitivity 96
Service Set Identity (SSID) 29, 38
signal strength 52, 54
site information 54
site survey 54
  scan 54
  security settings 55, 80
sleep mode 68
SSID 29, 38, 52, 54, 78, 93
statistics 52
syntax conventions 5
system tray 20

T

temperature 95
Temporal Key Integrity Protocol (TKIP) 41, 141
The 71
TLS 71, 73
total receive 52

total transmit 52
trademarks 179
Transmission rate 78
transmission rate 52, 64
transmit key 56, 81
transmit rate 52
trend chart 52, 53
TTLS 71

U

uninstalling the ZyXEL utility 86
upgrading the ZyXEL utility 87
  important step 87
user authentication 39
utility installation 20
utility version 86

V

Vista 71, 73

W

warranty 182
  note 182
weight 95
WEP 39, 56
  automatic setup 40
  manual setup 40, 57, 82
  passphrase 40, 56, 81
WEP (Wired Equivalent Privacy) 39
WEP Encryption 56
WEP key generation 40
Wi-Fi Protected Access 41, 140
Wi-Fi Protected Setup 51
Windows 71
Windows XP 21
Wired network 80
wireless client 38
wireless client WPA supplicants 142
wireless LAN
  introduction 37
  security 39
wireless LAN (WLAN) 37
wireless network 38
wireless security 136
wireless standard 95
Wireless station mode
  profile 62
wireless station mode
  adapter 68
  security settings 55, 80
  site survey 54
  trend chart 53
wireless tutorial 24
WLAN
  interference 133
  security parameters 144
WPA 41, 58, 71, 140
  key caching 142
  pre-authentication 142
  user authentication 142
  vs WPA-PSK 141
  wireless client supplicant 142
  with RADIUS application example 142
WPA2 41, 58, 71, 140
  user authentication 142
  vs WPA2-PSK 141
  wireless client supplicant 142
  with RADIUS application example 142
WPA2-Pre-Shared Key 41, 140
WPA2-PSK 41, 57, 82, 140, 141
  application example 143
WPA-PSK 41, 57, 82, 141
  application example 143
WPS
  see also Wi-Fi Protected Setup 51
WZC
  activating 157
  network connection 159
  not available 159
  preferred network 169
  security setting 163
  system tray icon 159
WZC (Wireless Zero Configuration) 21

Z

ZyXEL Utility
  accessing 21
ZyXEL utility 21
  accessing 21
  driver version number 86
  exiting 21
  help 22
  reactivating 21
  status 21
  system tray icon 20
  upgrading 87
  version number 86